54Mb Operator Access Point

P-520

User's Guide

Revision 2.0

April 8, 2004

www.gemtek-systems.com

Gemtek Systmes declares that P-520 (FCC ID: MXF-AP930301G) is limited in CH1~CH11 by □ specified firmware controlled in U.S.A.

Copyright

Notice

Gemtek Systems reserves the right to change specifications without prior notice.

While the information in this manual has been compiled with great care, it may not be deemed an assurance of product characteristics. Gemtek Systems shall be liable only to the degree specified in the terms of sale and delivery.

The reproduction and distribution of the documentation and software supplied with this product and the use of its contents is subject to written authorization from Gemtek Systems.

Trademarks

The product described in this book is a licensed product of Gemtek Systems Holding BV.

Microsoft, Windows 95, Windows 98, Windows Millennium Edition, Windows NT, Windows 2000, Windows XP, and MS-DOS are registered trademarks of the Microsoft Corporation.

Mac OS is a registered trademark of Apple Computer, Inc.

Java is a trademark of Sun Microsystems, Inc.

Wi-Fi is a registered trademark of the Wi-Fi Alliance.

All other brand and product names are trademarks or registered trademarks of their respective holders.

National Radio Regulations

The usage of wireless network components is subject to national and or regional regulations and laws. Administrators must ensure that they select the correct radio settings according to their regulatory domain. Refer to appendix **B) Regulatory Domain/Channels** for more information on regulatory domains. Please check the regulations valid for your country and set the parameters concerning frequency, channel, and output power to the permitted values!

FCC Warning

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation.

This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

FCC Caution

To assure continued compliance, any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment

FCC Radiation Exposure Statement

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator and your body. This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

R&TTE Compliance Statement

This equipment complies with all the requirements of the Directive 1999/5/EC of the European Parliament and the Council of 9 March 1999 on Radio Equipment and Telecommunication Terminal Equipment and the Mutual Recognition of their Conformity (R&TTE).

The R&TTE Directive repeals and replaces in the directive 98/13/EEC (Telecommunications Terminal Equipment and Satellite Earth Station Equipment) As of April 8, 2000.

Safety

This equipment is designed with the utmost care for the safety of those who install and use it. However, special attention must be paid to the dangers of electric shock and static electricity when working with electrical equipment. All guidelines of this manual and of the computer manufacturer must therefore be allowed at all times to ensure the safe use of the equipment.

EU Countries Intended for Use

This device is intended for home and office use in Austria, Belgium, Denmark, Finland, France (with Frequency channel restrictions), Germany, Greece, Ireland, Italy, Luxembourg, The Netherlands, Portugal, Spain, Sweden and United Kingdom.

The ETSI version of this device is also authorized for use in EFTA member states Iceland, Liechtenstein, Norway and Switzerland.

EU Countries Not Intended for Use

None.

Contents

About this Guide

Purpose

This document provides information and procedures on hardware installation, setup, configuration, and management of the Gemtek Systems 54Mbps Operator Access Point P-520.

Prerequisite Skills and Knowledge

To use this document effectively, you should have a working knowledge of Local Area Networking (LAN) concepts and wireless Internet access infrastructures. In addition, you should be familiar with the following:

- Hardware installers should have a working knowledge of basic electronics and mechanical assembly, and should understand related local building codes.
- Network administrators should have a solid understanding of software installation procedures for network operating systems under Microsoft Windows 95, 98, Millennium Edition, 2000, NT, and Windows XP and general networking operations and troubleshooting knowledge.

Conventions Used in this Document

The following typographic conventions and symbols are used throughout this document:

	Very important information. Failure to observe this may result in damage.
	Important information that should be observed.
	Additional information that may be helpful but which is not required.
bold	Menu commands, buttons and input fields are displayed in bold
`code`	File names, directory names, form names, and system-generated output such as error messages are displayed in constant-width type
<value>	Placeholder for certain values, e.g. user inputs

Help Us to Improve this Document!

If you should encounter mistakes in this document or want to provide comments to improve the manual please send the e-mail directly to:

manuals@gemtek-systems.com.

Gemtek Systems Technical Support

If you encounter problems when installing or using this product, please consult the Gemtek Systems website at:

http://www.gemtek-systems.com for:

- The latest software, user documentation and product updates.
- Frequently Asked Questions (FAQ).
- Direct contact to the Gemtek Systems support.

Chapter 1 – Introduction

Thank you for choosing the Gemtek Systems 54Mbps Operator Access Point model P-520.

The Gemtek Systems P-520 is a **Carrier-Grade Wi-Fi Access Point** designed to provide reliable and secure wireless access to an operator network or enterprise LAN. Theft-proof mounted to a wall or ceiling the access point can be fully configured and controlled from a central management system minimizing the need for an engineer to physically access the unit once it has been installed.

Product Overview

High Performance for Maximum Coverage

The Gemtek Systems P-520 Operator Access Point provides quality connectivity for Wi-Fi networks. Designed to support even the largest of Hot Spots, this AP combines high receiver sensitivity and proven antenna technology to maximize coverage.

Wi-Fi Compliance to Ensure Network Compatibility

Tested for interoperability with the Wi-Fi standard, the P-520 will support all Wi-Fi certified client devices; the global industry-standard for local wireless networking.

The Perfect Access Point for Large Areas

The P-520 is specifically designed for large venues. Connected to a Access Controller like the Gemtek Systems G6000 or P-560, P-520s can easily cover a hotspot of any size. P-520 is IEEE 802.3af compliant, enabling it to be powered over standard Cat-5 Ethernet cabling, reducing installation and maintenance costs.

Total Management

The P-520 Operator Access Point simplifies the set-up, operation, control and management of public access networks. The AP can be remotely managed via HTTP or SNMP. Auto-channel selection and integrated site survey utilities help administrators to optimize cell planning.

Security

P-520 supports various state-of-the-art security mechanisms like WPA, Access Control Lists, 802.1x/EAP authentication and Layer 2 User Isolation. The User Isolation feature can effectively prevent peer-to-peer communication between client stations. The AP is designed for wall mount with integrated theft-protection.

Management Options

There are several managing and monitoring interfaces available to the operator to configure and manage the P-520 on your network:

- Web-browser Interface
- SNMP Management (SNMP v1, v2c)

This user manual provides detailed description of Web and SNMP management option.

Web Interface

The Web-browser interface (also known as the HTTP interface) provides easy access to configuration settings and network statistics from any computer in the network. Use the Web browser interface through your LAN (switch, hub, etc.), over the Internet, or with a "crossover" Ethernet cable connected directly to your computer's Ethernet Port.

SNMP Management

In addition to the Web interface, you can also manage and configure a P-520 using the Simple Network Management Protocol (SNMP). SNMP enables network administrators to manage network performance, find and solve network problems, and plan for network growth.

In order to manage the device you have to provide your Network Management System software with adequate MIB files. Please consult your management software manuals on how to do that.

P-520 Features

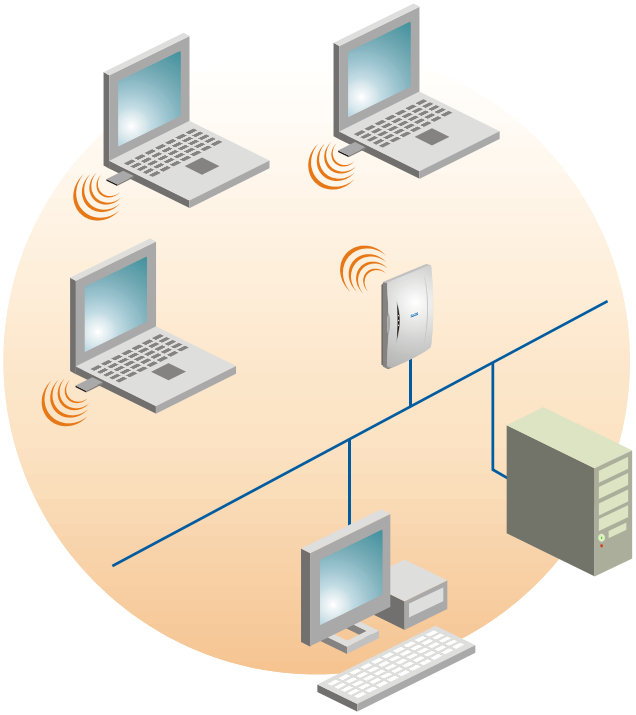
- IEEE 802.11g/b Access Point,
- Wi-Fi certified
- Integrated high-gain diversity antennas
- Adjustable output power, up to 20dBm
- Power-over-Ethernet support, IEE 802.3af compliant
- Theft protection system
- 802.1x/EAPoLAN
- WPA (PSK, TKIP)
- Seamless roaming (IAPP support)
- Virtual local area network support (VLAN)
- Remote management, remote updates
- Layer 2 Isolation (disable peer-to-peer traffic)
- ACL (Access Control List)
- DHCP client
- Remote software update
- SNMPv1, SNMPv2, incl. traps, MIB-II, IEEE-802.11, Gemtek general Private MIB

Operating Modes

The P-520 Access Point can work in different operating modes:

- **Access Point (AP) mode:**

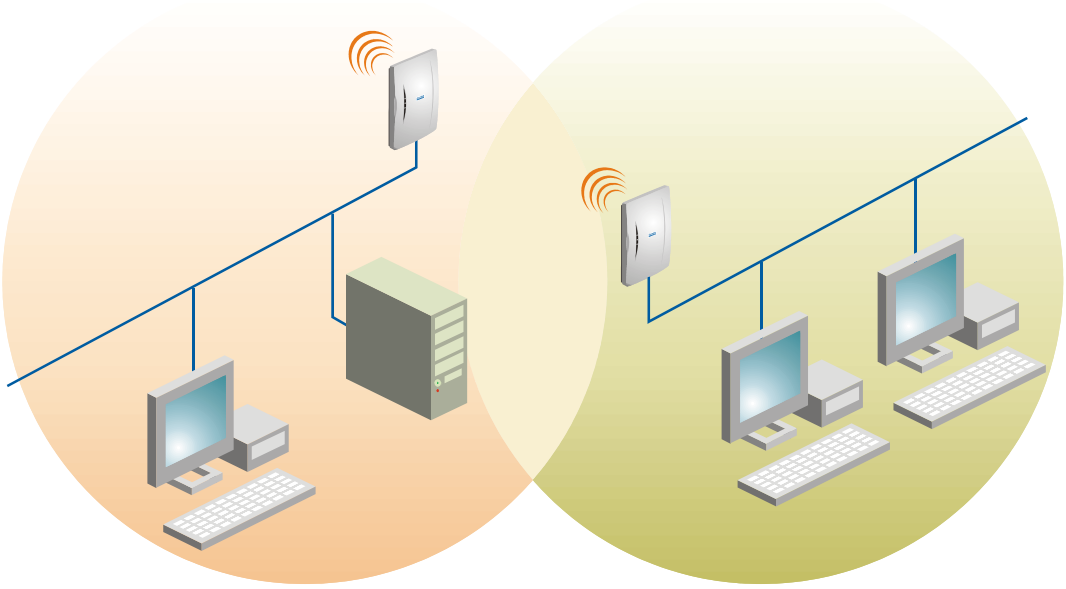
In AP mode the P-520 can connect multiple wireless client stations to a wired network. The Local Area Network and the Wireless Network are from the same IP address space.



- **Access Point with WDS (Wireless Bridge and Wireless Repeater) mode:**

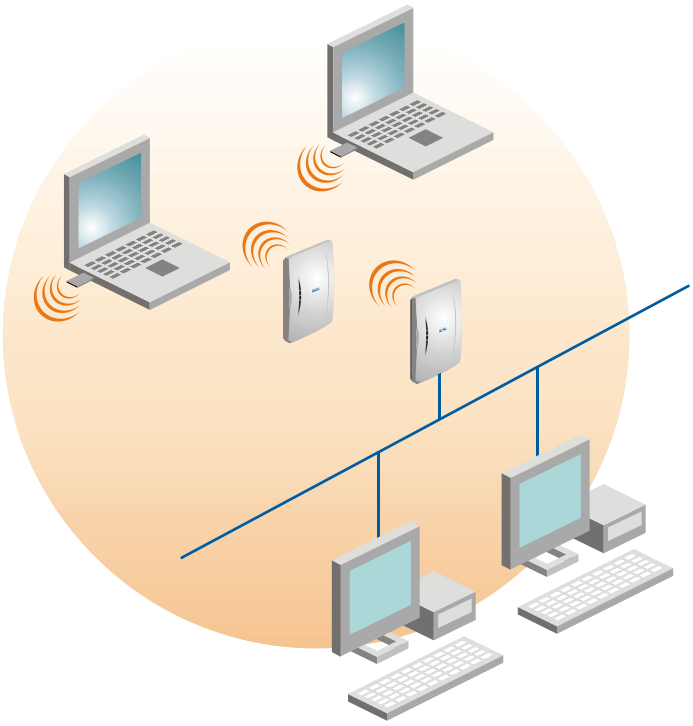
A **WDS (Wireless Distribution System)** allows you to create a wireless network infrastructure. Normally, the access points must be connected with a wire (LAN), which is generally an Ethernet connection in business applications. Once connected, these access points create wireless cells allowing a wireless connection. The WDS feature allows the access points to be wirelessly connected to another access point, eliminating the need to the wired connection between them. Two WDS configurations are described in the following pictures: **wireless bridge** and **wireless repeater**.

Wireless Bridge:



The first use of the **WDS, Wireless Bridge** mode is to create the wireless bridge between two or more wired networks, for example networks in different buildings with no wired connections between them. All APs in a WDS have to be configured for the same radio channel and must be configured with their WDS partner AP BSSIDs (MAC addresses). The data being transported is bridged transparently; i.e., the data received by the LAN station is identical to data that would be received if both LAN stations had been connected to the same LAN subnet.

Wireless Repeater:



The other use of the **WDS, Wireless Repeater** mode is to extend wireless area coverage between wired and wireless networks. This mode is normally used in large, open areas, where pulling a wire is prohibited or not cost effective and in residential circumstances. By settings up the BSSIDs (MAC addresses) between AP's WDS partners, stations can intersect with any AP of this BSSID and move between the coverage of both APs.

In both cases, the P-520 acts as a network bridge between wireless and wired networks. All data received by the P-520 on its wireless or Ethernet interface is broadcast on the wireless interface to all connected devices that are authorized in the ACL (access control list).

Antenna Diversity

The P-520 Operator Access Point uses antenna diversity to select the best reception signal at the two integrated antennas. Antenna diversity counters the adverse effects of multi-path fading and antenna pattern nulls and reduces the packet error rate.

The main antenna (at internal connector J4) is used for transmission whereas both antennas, main and aux, can receiving signals. Receive diversity examines only packets directed at the AP. A count of frames received consecutively with FCS errors is compared to the configured threshold value. When this value is reached, the receive antenna used is switched to the other antenna. If a directed frame is received without errors the error count is reset back to zero.

Chapter 2 – Installation

This chapter provides installation instructions for the hardware and software components of the P-520 Operator Access Point. It also includes the following information:

- **The Packaging Contents**
- **System Requirements**
- **Hardware Introduction**
- **Hardware Installation**

The Packaging Contents

Each Operator Access Point comes with the following:

- Wireless LAN Access Point P-520
- Wall mounting clamp
- Tool for disassembling the housing
- Twisted pair LAN cable
- Power Adapter
- Installation CD containing software and documentation:
  - P-520 User Guide in PDF format
  - Release Note
  - KickStart Utility
  - Product Firmware
  - Adobe Acrobat Readers
- Warranty Card

If any of these items are missing or damaged, please contact your reseller or Gemtek Systems sales representative.

System Requirements

The management of the P-520 is independent of your operating system. You will need a computer that is connected to the same IP network as the P-520 (via Ethernet) and the HTML browser (e.g. Internet Explorer, Netscape, Opera).

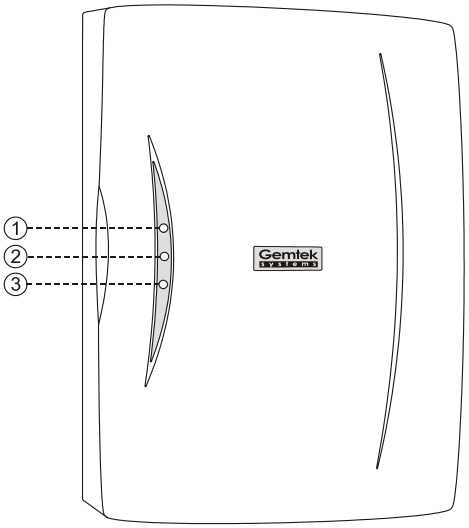
A Windows operating system is required for installing and using the KickStart utility delivered with the product CD.

For setting up the integrated 802.1x/EAP based access control function, you need to provide a connection to a Gemtek Systems access controller or a 3rd party RADIUS server.

Hardware Introduction

Front Panel: LEDs

The Operator Access Point has three LED's located on its front.



1. Power LED

2. LAN link LED

3. Wireless activity LED

Figure 1 – P-520 LED's

Item	LED	Color	Status	Indication
1	Power LED	Green	Off	Power supply connection not available or broken
			On	Power supply connection OK
2	LAN Link LED	Green	Off	No LAN connection available
			On	LAN connection OK
3	Wireless activity LED	Green	Off	No activity
			Blinking	Sending and receiving data

Rear Panel

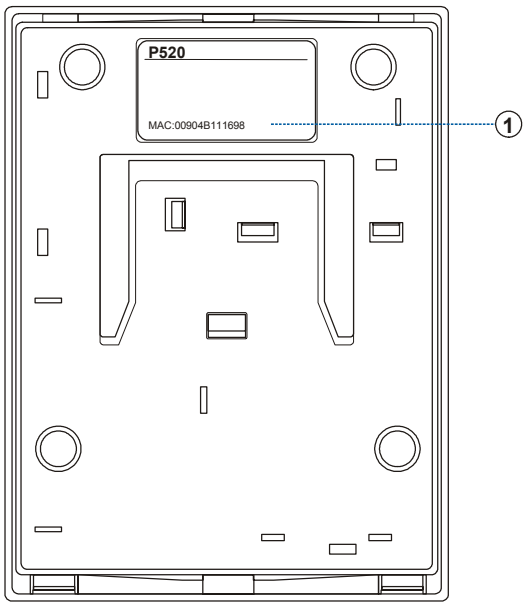


Figure 2 – Rear Panel of the P-520

1. MAC Address of the P-520

This label shows the **Wireless LAN MAC** which coincide with **LAN MAC** address of the device. You can determine the **Wireless LAN MAC** address by using the **KickStart.**

A Look Inside

Open the housing of the Access Point by pressing the spring latches on the bottom back side of the access point as shown:

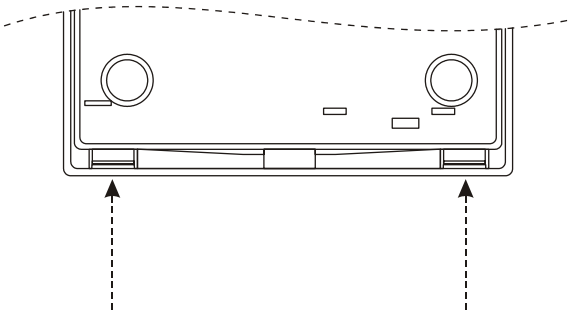
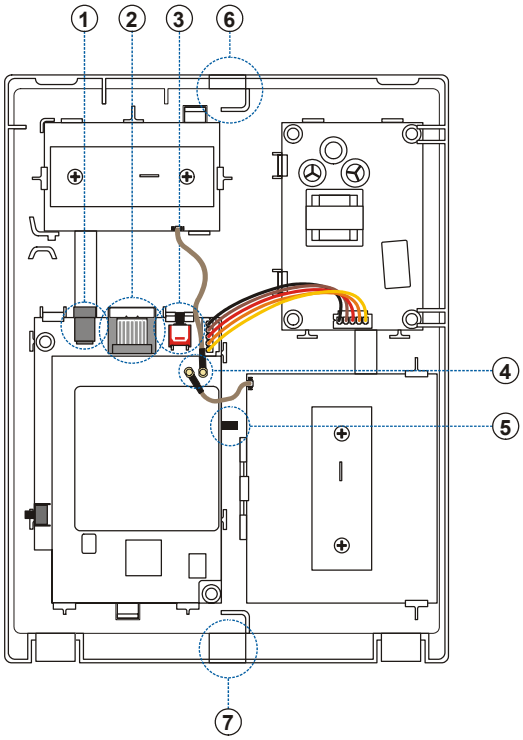


Figure 3 – Opening the P-520 Housing

Looking inside the P-520 you will find some important points:



1. Power Connector Plug for external 5V DC power supply. For use only when Power-over-Ethernet is not available. We advise to use either the external 5V power supply OR Power-over-Ethernet but not both in parallel.

2. Ethernet Socket for common twisted pair or Power-over-Ethernet cable.

3. Reset button: press 1 second to unlock the Access Point and to set the administrator's password to default. Press more than 8 seconds to reset the Access Point to factory default.

4. MMCX Antenna Connectors for internal and external antennas is the J4 connector. For use with original Gemtek Systems antennas and antenna cables only!

5. After installing the Access Point on the wall, release the spring latch to *Removing the Access Point from the Wall.*

6. Top Cable Inlet for Ethernet cable or antenna cable for additional external antennas.

7. Bottom Cable Inlet for Ethernet cable or antenna cable for additional external antennas.

Figure 4 – Looking Inside the P-520

You can feed the Ethernet cable, external power supply or antenna cable for additional external antennas in two ways:

- Through the top cable inlet
- Through the bottom cable inlet

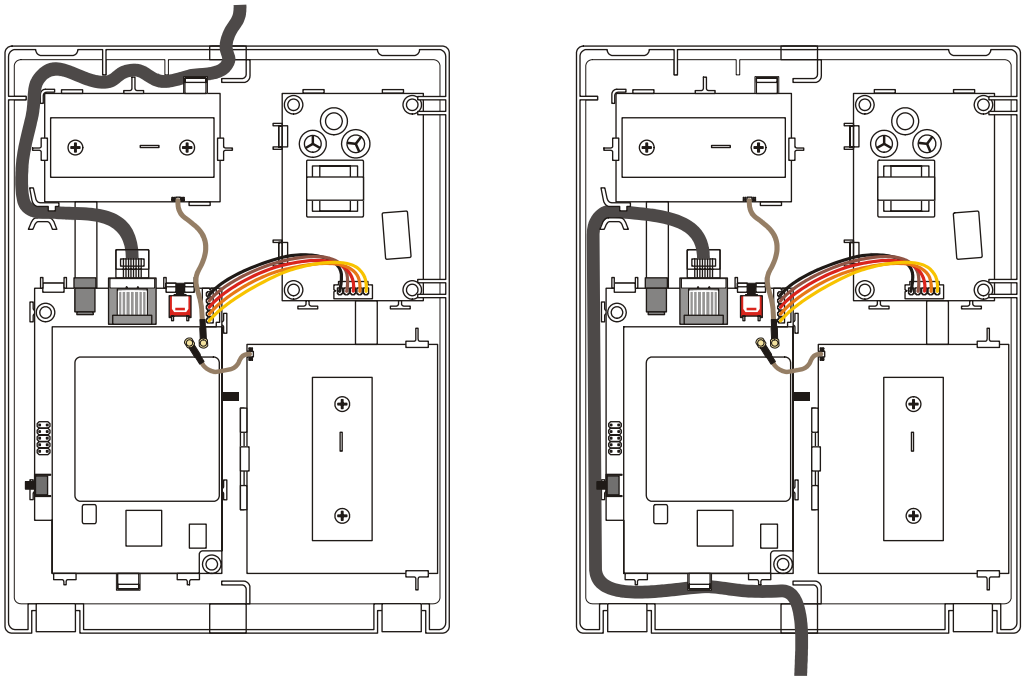


Figure 5 – Top and Bottom Cable Inlet of the P-520

Hardware Installation

Carefully select the ideal position for your Access Point by considering the following recommendations:

- The length of the Ethernet cable that connects the Access Point to the network must not exceed 100 meters.
- Place the Access Point in a dry, clean location as far from the ground as possible, such as at the top of a wall, keeping clear of metal obstructions.
- Place the Access Point away from transformers, heavy-duty motors, fluorescent lights, microwave ovens, refrigerators, or other equipment that could cause radio signal interference.
- Locate the AP(s) so that the primary lobe provides coverage where it is required.
- Don't cover the Access Point with material that absorbs the radio signal (e.g. wooden paneling, walls).

Attaching the Access Point to the Wall

Step 1 Place the Access Point at the desired location. Use the wall mounting assembly kit that is delivered with the P-520 Access Point.

Step 2 Attach the wall mounting clamp to the wall with the spring latch to the upper side using the four screws.

Step 3 Connect the rear side of the Access Point to the mounting plate:

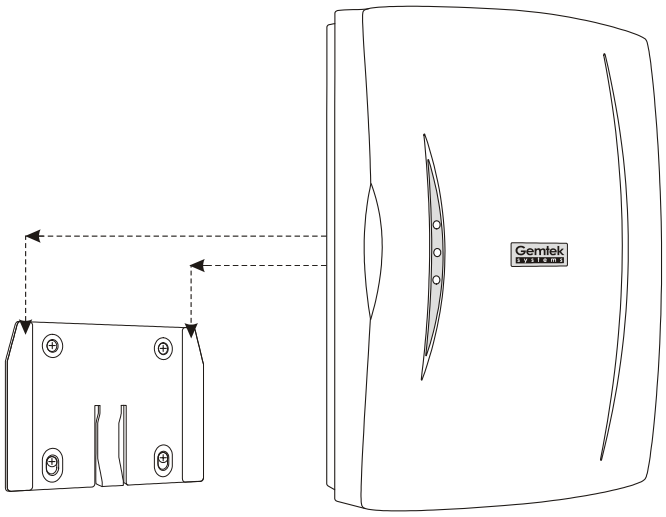


Figure 6 – Attaching the P-520 Housing to the Mounting Clamp

Step 4 Move the housing slightly downward and press until the spring latch is locked in place. The P-520 Access Point is now securely mounted onto the wall and cannot be removed without special tools.

Step 5 Open the housing of the Access Point and connect an Ethernet cable to the RJ45 socket. Run the cable to the desired cable inlet then close the housing.

Step 6 Connect the twisted pair LAN cable to a Power-over-Ethernet device (switch or injector). At least the power LED and the LAN link LED should light up.

Removing the Access Point from the Wall

Step 1 Open the housing of the Access Point by pressing the spring latches on the upper rear side of the access point using the disassembling tool delivered with your P-520:

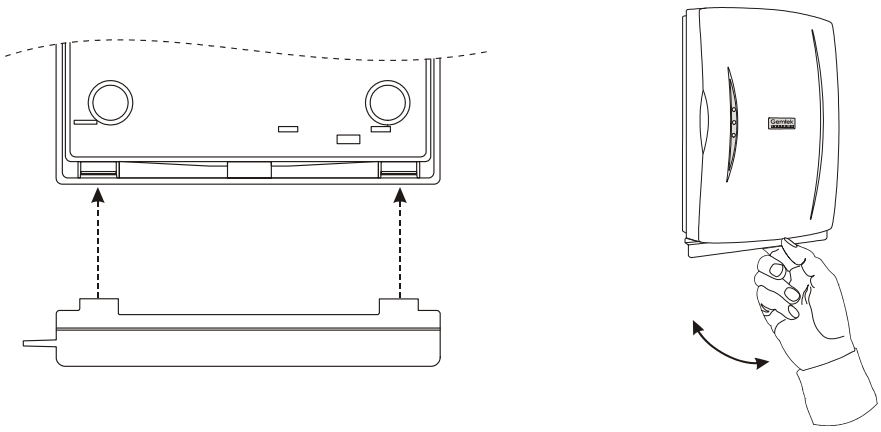


Figure 7 – Removing the P-520 Housing Using the Disassembling tool

Step 2 Release the housing from the wall-mounting clamp by carefully pressing the spring latch in the center of the device (unit 5 in the

Figure 4 – Looking Inside the P-520) using the point of the disassembling tool:

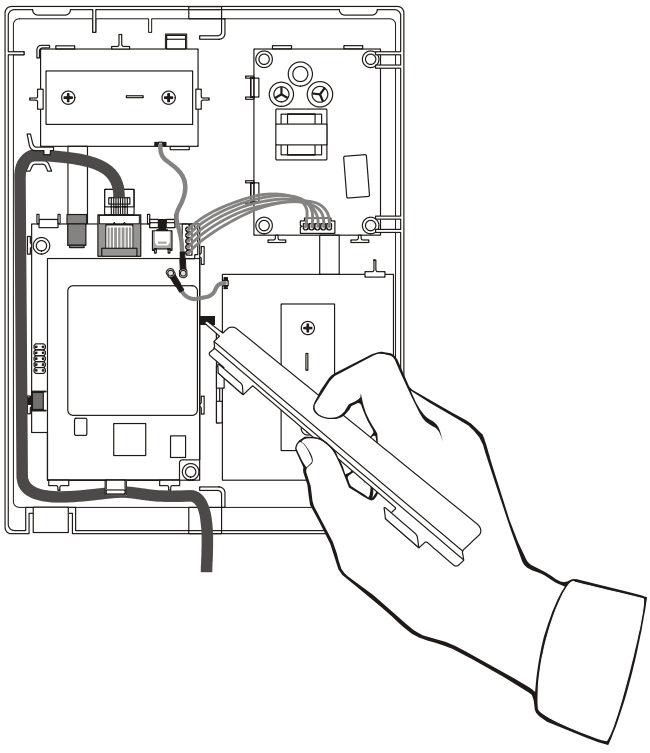


Figure 8 – Releasing the P-520 Housing

Step 3 Move the housing slightly upward and remove it.

Initialization

The following paragraphs describe how to access the web configuration interface of the Gemtek Systems P-520. After unpacking and connecting the product for the first time it responds to a dynamic IP address given by your local DHCP server. To locate the dynamic IP address of the P-520 use the KickStart utility.

Software Introduction: KickStart

The Gemtek Systems **KickStart** is a software utility that is included on the Product CD.

The utility automatically detects Gemtek Systems access points installed on your network, regardless of its IP address, and lets you configure each unit's IP settings. The feature list for the **KickStart** utility is listed below:

- Scanning your network for all network devices
- Quick access to your AP via http, https, telnet, ssh
- Setting new IP address of your AP
- Reset to factory default settings
- Default access (in case of lost administrator password)
- Firmware updates

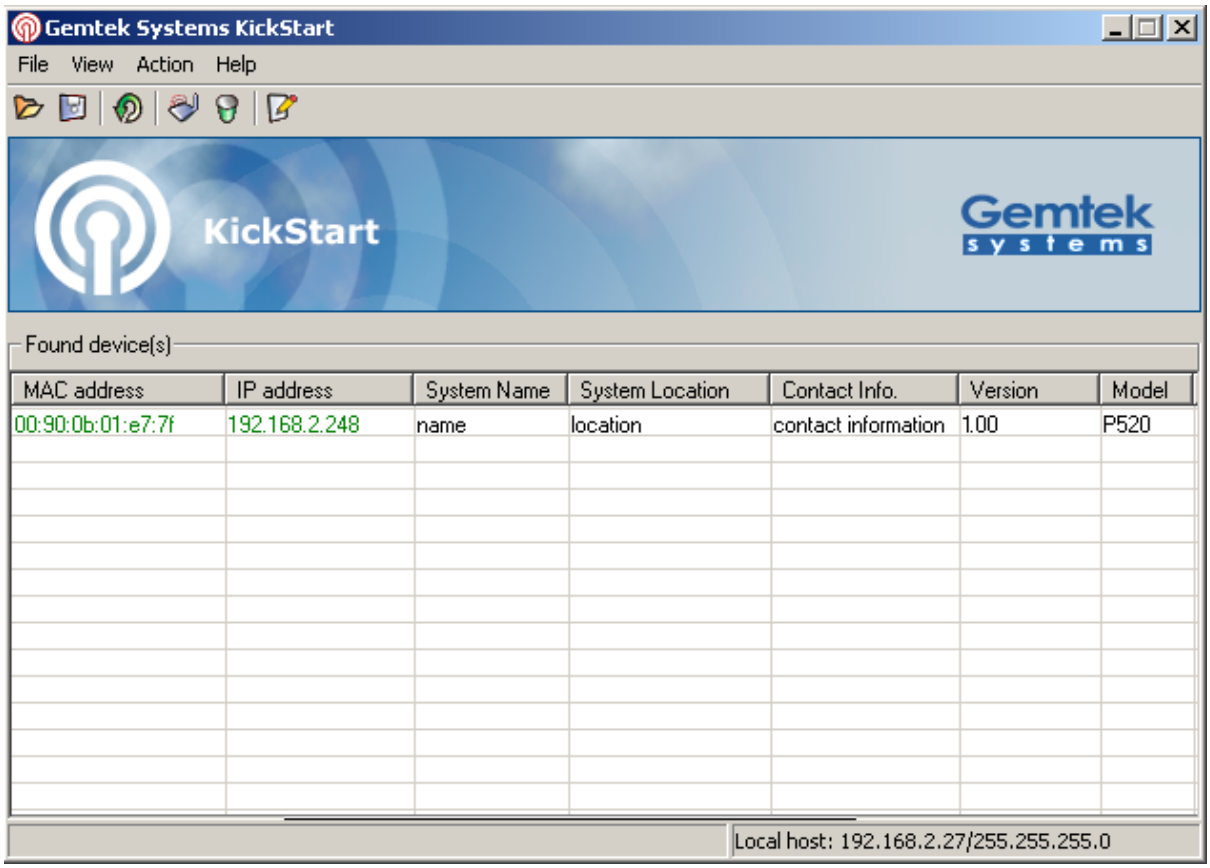
To install the **KickStart** utility insert the Installation CD into your CD-ROM drive. Find and install the utility from the product CD into the computer.

If the Installation CD does not start automatically, please run "**autorun.exe**" manually from the root directory of the installation CD.

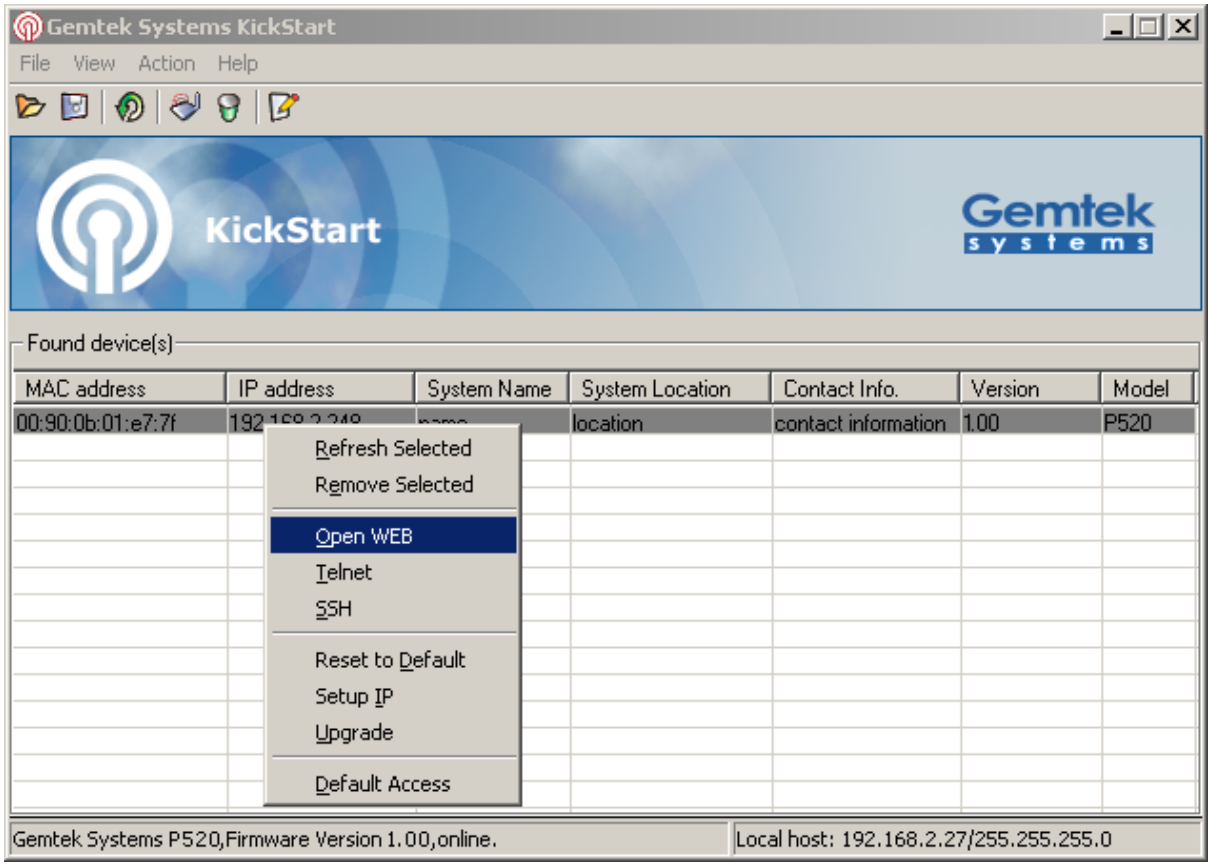
Access your P-520 Access Point

In default configuration your access point IP address is assigned by the DHCP server so for the first web browser connection to your AP launch the **KickStart** utility that is provided with your product CD and follow the instuctions

Step 1 Install the **KickStart** utility from the **Installation CD**. Click **Start > Programs > Gemtek Systems > KickStart** to launch the application. If the P-520 is connected to your network, the utility will automatically find your device:



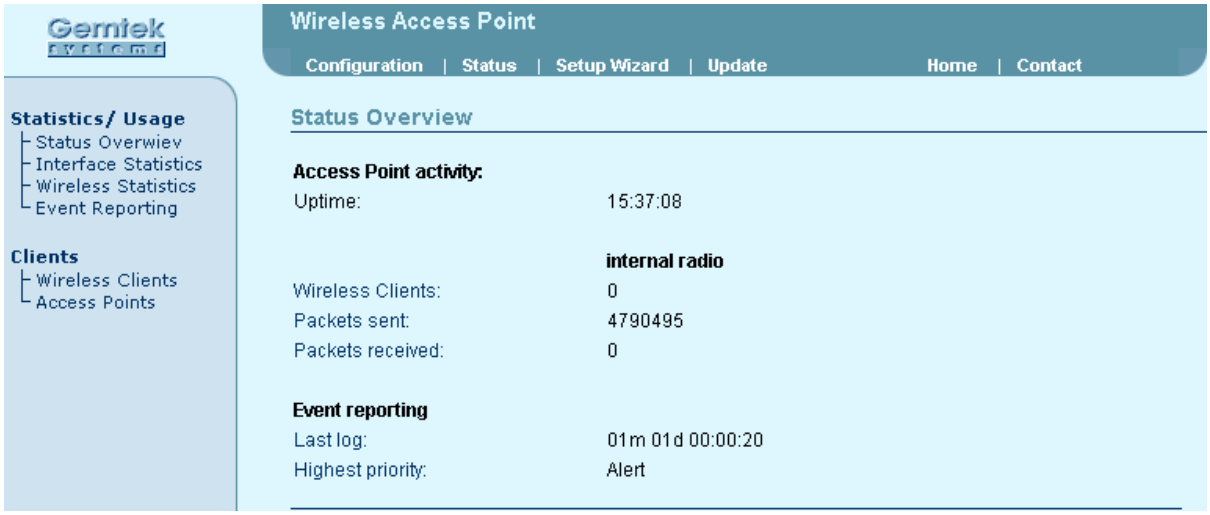
Step 2 Select your access point and right click. Select **Open WEB** item to launch the web management interface through the http connection:



Step 3 Enter the P-520 administrator login details to access the web management interface.

The default administrator log on settings for all access point interfaces are:
User Name: **admin**
Password: **admin01**

Step 4 After successful administrator log on you will see the main page of the access point's **web interface**:



In the center of the screen a menu is displayed with links to the six different setup areas:

- **Configuration**
- **Status**
- **Setup Wizard**
- **Update**
- **Home**
- **Contact**

You can now perform the initial access point configuration.

Reset to the Factory Default Settings

Keep in mind that resetting the device is an irreversible process. Please note that even the administrator password will be set back to the factory default!

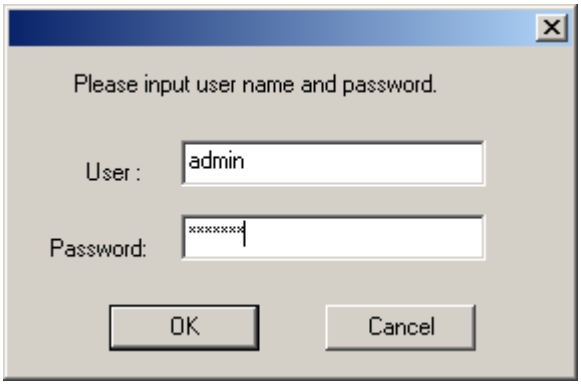
If you have mis-configured your device in such a way that you cannot get access to modify its parameters via your Web browser you have two options to reset the device back to its factory default settings.

- Method one requires access to the internal **Reset Button** (item 3, in
- *Figure 4 – Looking Inside the* P-520) as described in chapter: **Hardware Introduction**.
- The second option is using the **KickStart** utility provided on the product CD. Note, that the KickStart utility finds you access point is in the different subnet than your computer. To reset the AP using **KickStart** follow the guideline below:

Step 1 Find you P-520 according the **Ethernet MAC** (Media Access Control) address in the **Found Devices** table. The **Ethernet MAC** address is the serial number of the P-520 decremented by 1 (in hexadecimal).

Step 2 Select your access point and right click. Select **Reset to Default** item to set your device back to the factory defaults.

Step 3 Enter the P-520 administrator login details as requested and click OK:



Step 4 After successful administrator log on your access point will set back to the default status.

Refer to the appendix, section: **C) Factory Defaults Values for the P-520 Access Point** for a detailed list of factory default values.

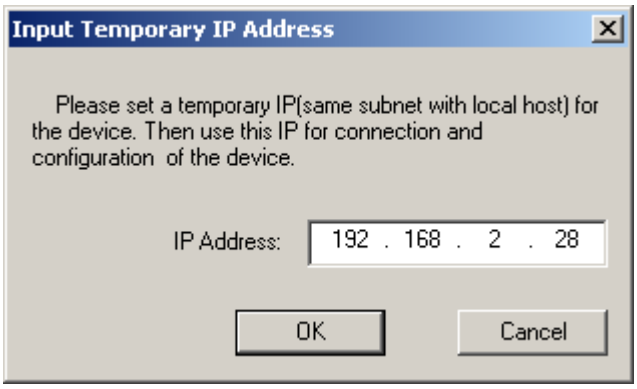
You can reset your AP even if the administrator password is lost. Use the **KickStart** utility to access your AP with the default administrator account (login: admin, password: admin01). Follow the guidelines below:

This default access function is available only **1 minute** after the access point reboot.

Step 1 Find you P-520 according the **IP address** or **Ethernet MAC** (Media Access Control) address in the **Found Devices** table. The **Ethernet MAC** address is the serial number of the P-520 decremented by 1 (in hexadecimal).

Step 2 Select your access point and right click. Select **Default Access** item to access your device with default administrator settings.

Step 3 Enter the **Temporary IP Address** for your AP, e.g. 192.168.2.28 (address should be from the same subnet as local host) and click the OK:



Step 4 After successful entry of a temporary IP address you can access your access point with the default administrator login. The access point system configuration (except temporary IP address) is left unchanged.

Chapter 3 – Quick Setup

This chapter provides how to setup the P-520 Operator Access Point the step-by step.

Setup Wizard

To easily configure your access point step-by-step, choose the **Setup Wizard** from the main menu. With this wizard you are able to configure the following settings:

- Select the country and regulatory domain in which you will use the access point
- Specify IP addresses (static or dynamic)
- Define the radio policy (802.11b, 802.11g or Mixed)
- Specify the network name (SSID) and the radio channel
- Choose the wireless security settings (No encryption, WEP, WPA)
- Configure the administrator's password

Figure 9 – Main Menu

Click **Setup Wizard** on the top menu and follow the instructions of the **Basic Setup Wizard**. Click the **Next** button and a new page with country selection appears.

Step 1 Country Selection

When **County Selection** page is displayed you can choose the country in which this access point will be used. Just choose country from drop-down list:

Figure 10 – Country Selection

Back – click return to the main wizard page.

Next – click to continue the access point setup process.

Cancel – click to cancel the access point setup process.

To continue the setup wizard click the **Next** button and choose the primary address selection.

Step 2 Network Setup

The IP configuration as described below is required for device management purposes. IP addresses can either be retrieved from a DHCP server or configured manually.

To setup the device IP configuration manually, choose the **Static IP** radio button and enter the credentials:

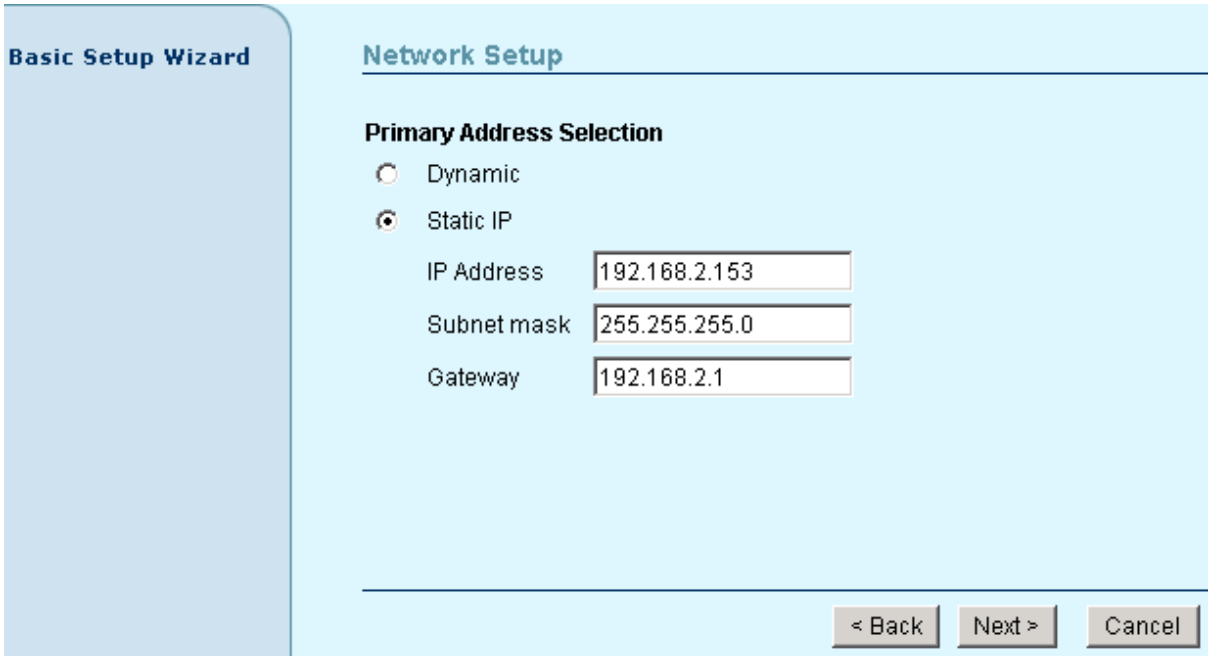


Figure 11 – Network Setup Settings

IP Address – specify the access point's IP address [digit and dots]. When shipped from the factory or reset to factory settings, the AP defaults to a static IP address of 192.168.2.2.

Subnet Mask – specify the access point's subnet mask [digit and dots]. When shipped from the factory or reset to factory settings, the AP defaults to a subnet mask of 255.255.255.0.

Gateway – specify the IP address of the access point's gateway [digit and dots]. When shipped from the factory or reset to factory settings, the AP defaults to a gateway IP address of 192.168.2.1.

Select **Dynamic** radio button, if need that IP address should be assigned by the DHCP server. The static IP settings are displayed but have no affect on the network configuration:

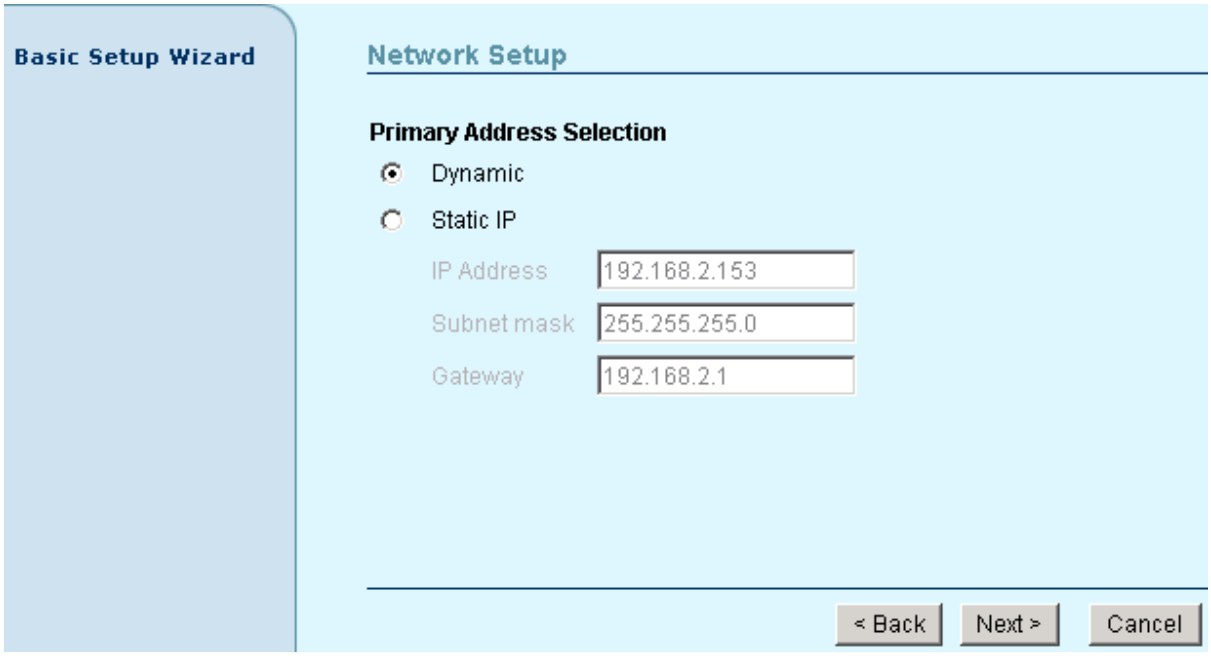


Figure 12 – Network Setup

To find your P-520 with dynamic IP settings use the KickStart.

Back – click return to the previous wizard page.

Next – click to continue the access point setup process.

Cancel – click to cancel the access point setup process.

Step 3 Internal Radio Policy

When the IP configuration is finished click the **Next** button and new page **Internal radio policy** is displayed. You can choose now the radio policy. It can be G-only (802.11g), B-only (802.11b) or Mixed (allows both 802.11b and 802.11g):

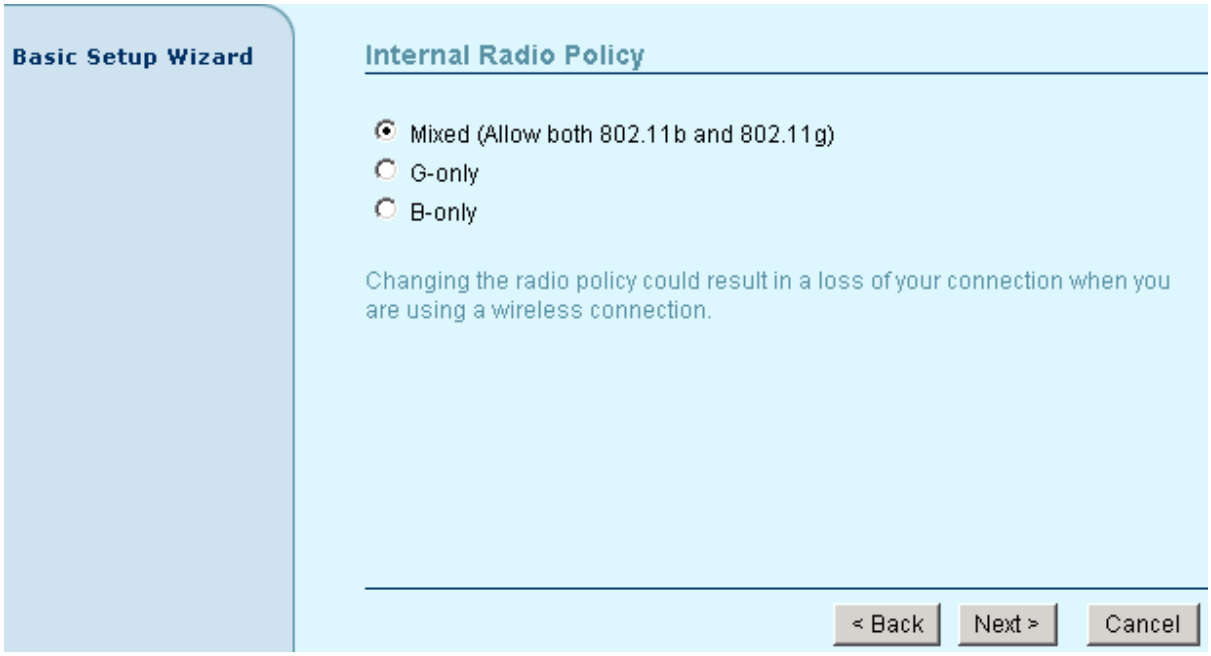


Figure 13 – Internal Radio Policy Settings

Changing the radio policy could result in a loss of your connection when you are using a wireless connection.

Mixed – select the mixed radio policy that allows both 802.11b and 802.11g modes.

G-only – select the 802.11g mode to connect 802.11g clients only.

B-only – select the 802.11b mode to connect 802.11g clients only.

Back – click return to the previous wizard page.

Next – click to continue the access point setup process.

Cancel – click to cancel the access point setup process.

To continue the setup wizard click the **Next** button.

Step 4 Network Identification

When the radio policy is chosen according your needs, you need to specify the **Network identification** settings of your wireless LAN. You can enter now the SSID and choose the radio channel:

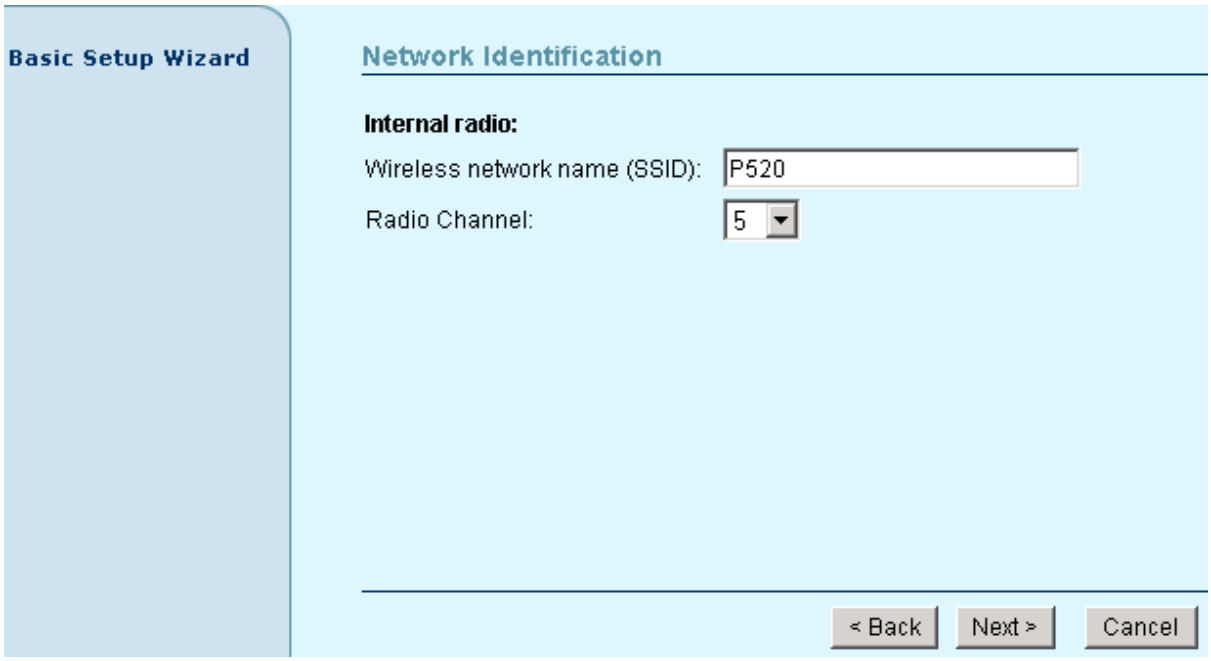


Figure 14 – Network Identification Settings

Wireless Network Name (SSID) – specify the unique name for your wireless network.

Radio Channel – select the channel that the access point uses to transmit and receive information.

Back – click return to the previous wizard page.

Next – click to continue the access point setup process.

Cancel – click to cancel the access point setup process.

More about SSID and Radio channel settings see the respective chapter:
Configuration | Wireless | Basic Settings

To continue the setup wizard click **Next** button.

Step 5 Security

Choose the security method to protect your data that only authorized network users could access the network. You can choose **WEP**, **WPA** or **No** security for your device.

If no security is needed, simply choose the **No Security** radio button:

Figure 15 – Security Settings

Back – click return to the previous wizard page.

Next – click to continue the access point setup process.

Cancel – click to cancel the access point setup process.

If you ant to choose WEP encryption, just select the **Wired Equivalent Privacy (WEP)** radio button and click **Next** button to configure the WEP encryption settings. You can then choose the encryption key length:

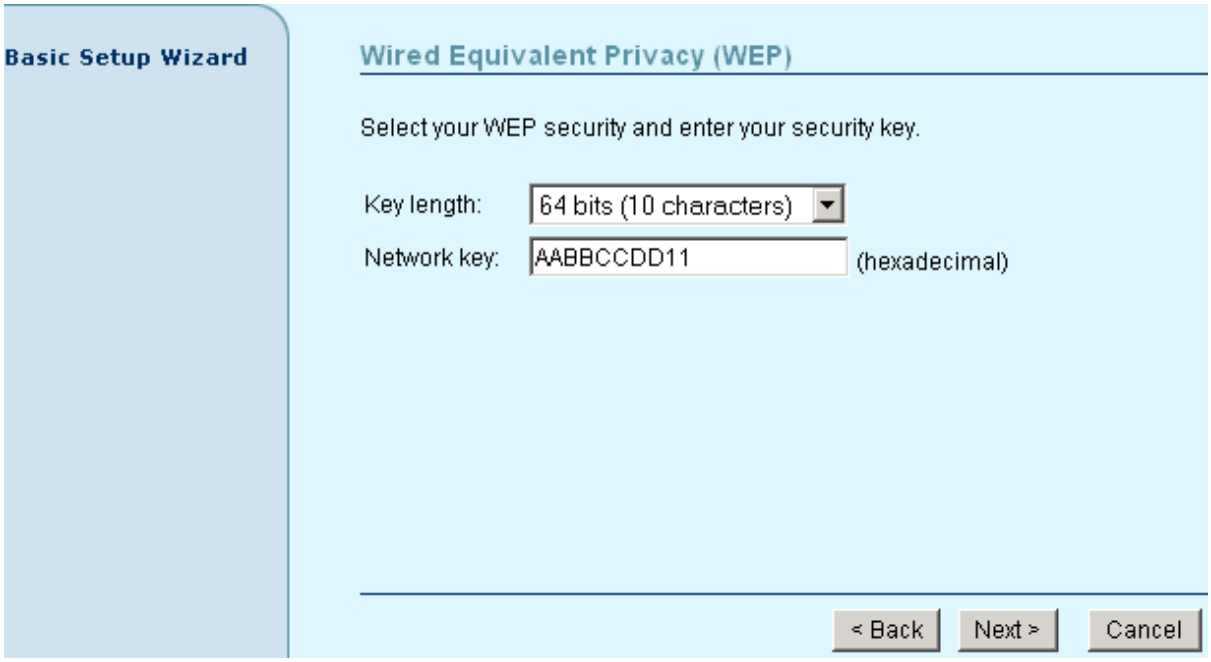


Figure 16 – WEP Encryption Settings

Key Length – choose the shared secret's Key length from drop-down list [64-bits (10 characters)/ 128-bits (26 characters)].

Network Key – specify the shared secret. 5 colon-separated HEX (0-9, A-F, and a-f) pairs (e.g. 00:AC:01:35:FF) for the 64-bits WEP encryption; 13 colon-separated HEX (0-9, A-F, and a-f) pairs (e.g. 00:11:22:33:44:55:66:77:88:99:AA:BB:CC) for the 128-bits WEP encryption.

Back – click return to the previous wizard page.

Next – click to continue the access point setup process.

Cancel – click to cancel the access point setup process.

To continue the setup wizard click the **Next** button and the new **Administrator Password Setup** page will appear.

More about WEP settings see the respective chapter: **Configuration | Security | Wireless Security | Wired Equivalent Privacy (WEP**)

If you want to choose WPA encryption, just select the **Wi-Fi Protected Access (WPA)** radio button in the **Security** page and click the **Next** button to configure the WPA encryption settings. You can now specify the WPA password phrase:

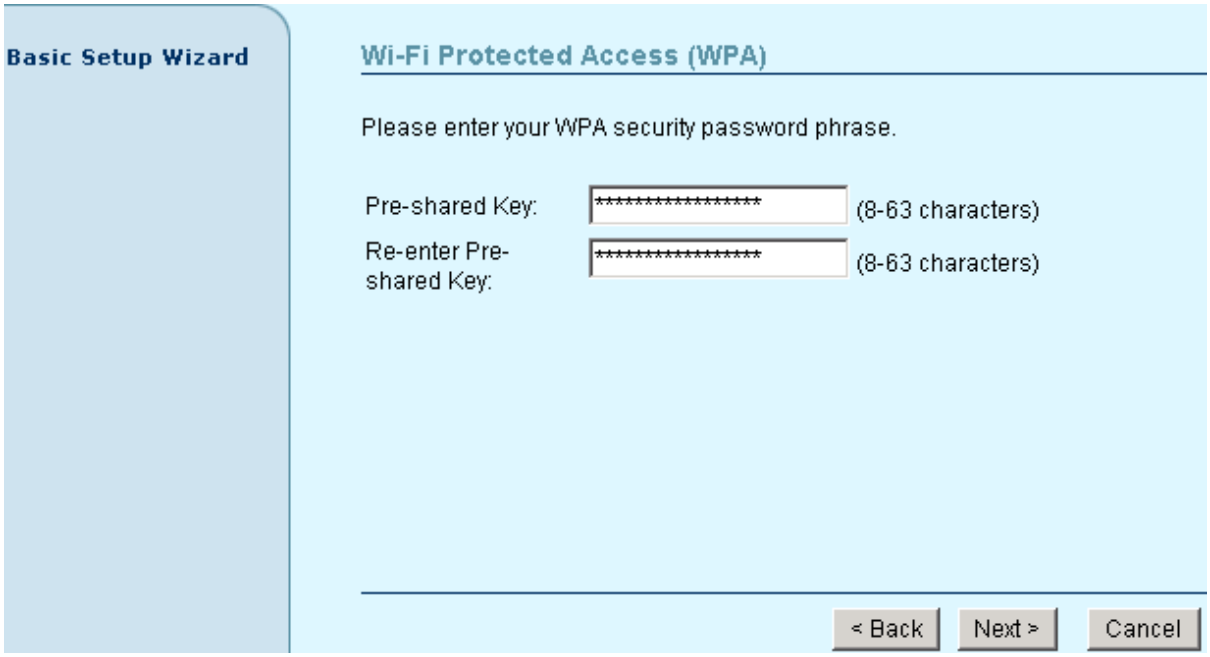


Figure 17 – Wi-Fi Protected Access (WPA) Settings

Pre-shared Key – specify WPA pre-shared key [8-63 characters].

Re-enter Pre-shared Key – re-enter the WPA pre-shared key to verify its accuracy [8-63 character].

Back – click return to the previous wizard page.

Next – click to continue the access point setup process.

Cancel – click to cancel the access point setup process.

To configure WPA without pre-shared key but with dynamic key exchange via RADIUS refer to the chapter **Configuration** | Security | Wireless Security | Wi-Fi Protected Access (WPA)

Step 6 Administrator Password Setup

After the security settings have been configured successfully click the **Next** button and the final step **Administrator Password Setup** will be displayed. Here you can choose and modify the administrator password to protect your AP from unauthorized configuration.

If you want to protect your access point from unauthorized access and configuration, select the **Use password protection** checkbox and specify a password:

Figure 18 – Administrator Password Setup Settings

Password – enter the new password value used for user authentication in the system [4-32 symbols].

Confirm Password – re-enter the new password to verify its accuracy.

Back – click to return to the main wizard page.

Next – click to continue the access point setup process.

Cancel – click to cancel the access point setup process.

Step 7 Confirm Settings

When Administrator's password configuration is finished, click the **Next** button to finish the Setup Wizard. You just need to confirm that settings are correct:

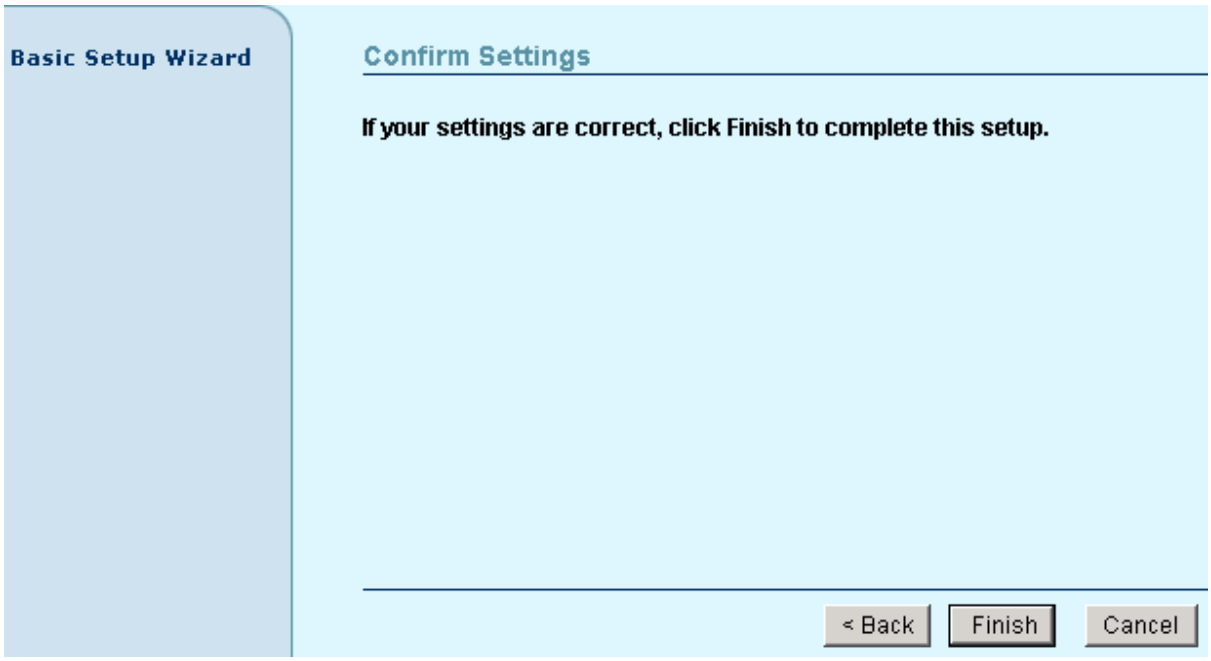


Figure 19 – Confirm Settings

Back – click to return to the previous wizard page.

Finish – click to finish the access point setup process.

Cancel – click to cancel the access point setup process.

Click the **Finish** button to complete the quick setup wizard. The Access Point is now ready for basic operation. You can now use the web interface menu to configure many more details for your P-520.

Chapter 4 – Reference Manual

The following paragraphs describe capabilities and configuration parameters of the web management interface of the P-520 Operator Access Point. When the access point is installed you can access and configure the device using a standard web browser.

This chapter includes the following subsections:

- **Configuration** – to configure essential access point settings: identity, network setup, VLAN, wireless settings, advanced wireless settings, wireless security, unauthorized configuration settings, download/upload backup configuration, reset device to defaults.
- **Status** – to view the system summary, interface statistics, wireless settings, event reporting, to find connected clients.
- **Setup Wizard** – quick device setup wizard.
- **Update** - device firmware update wizard.
- **Home –** click and you will be redirected to the main Status Overview page.
- **Contact –** click to view contact information.

Web Interface

The main menu of the **web management** is displayed at the top of the page after successfully logging into the system (see the figure below). From this menu all essential configuration pages can be accessed.

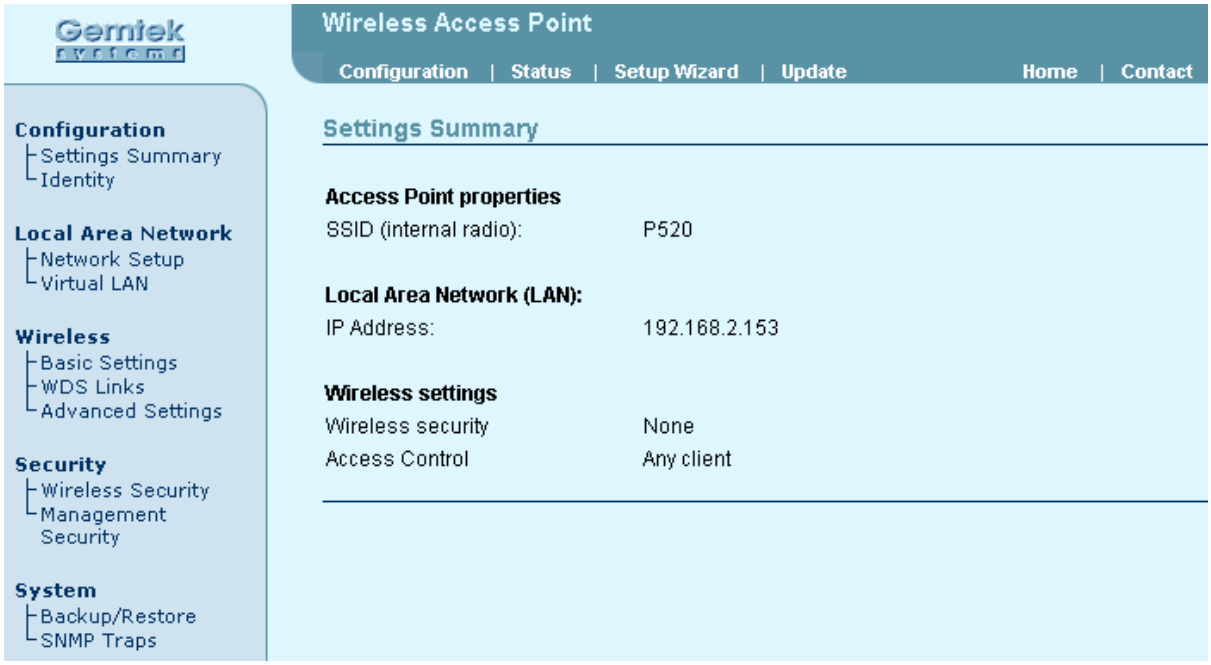


Figure 20 – Web Management Menu

By default the **Status** menu is activated and the current AP **Status Overview** page is displayed.

The **web management** menu has the following structure:

Configuration

Configuration – identity data of the access point:
- **Settings Summary –** the summary of main access point settings
- **Identity –** name, location, operator of the access point

Local Area Network – network interface configuration:
- **Network Setup** – IP address, netmask, gateway, Dynamic IP (DHCP)
- **Virtual LAN** – VLAN settings

Wireless - wireless interface configuration:
- **Basic Settings** – country selection, IAPP, SSID, band, channel selection, output power and other settings
- **WDS Links** – configuration of Wireless distribution Systems (bridge links)
- **Advanced settings** – advanced wireless settings

Security – access point security settings:
- **Wireless Security** – configure wireless security settings:
  - **Client Isolation** – deny or grant access between clients
  - **Access Control List (ACL)** – access control default policy, static ACL, access control by MAC address
  - **RADIUS Servers** – RADIUS servers IP, port and other settings
  - **Wired Equivalent Privacy (WEP)** – WEP security
  - **802.1x Security** – 802.1X network authentication
  - **Wi-Fi Protected Access (WPA)** – WPA security (encryption and authentication)
- **Management Security** – configure access of your access point

System – access point system settings:
- **Backup/Restore** – reset configuration to factory defaults values and/or reboot, download or/and upload system backup configuration
- **SNMP Traps** – SNMP traps settings

Status

Statistics/Usage – view system status:
- **Status Overview** – the summary of the access point status
- **Interface Statistics** – Local Loopback, LAN Ethernet, Internal Radio, WAN Ethernet statistic
- **Wireless Statistics** – wireless statistics
- **Event Reporting** – the log of important events

Clients – scan for access points and connected clients:
- **Wireless Clients** – connected users' statistics list
- **Access Points** – discover access points with internal radio
- **WDS Links** – WDS links' statistics

Setup Wizard

Update

In the following sections, short references for all menu items are presented.

Configuration

Configuration | Configuration | Settings Summary

The Settings Summary page shows important information of the P-520: its IP address, SSID, wireless security settings and access control status. The page is not configurable but displays the current system configuration only.

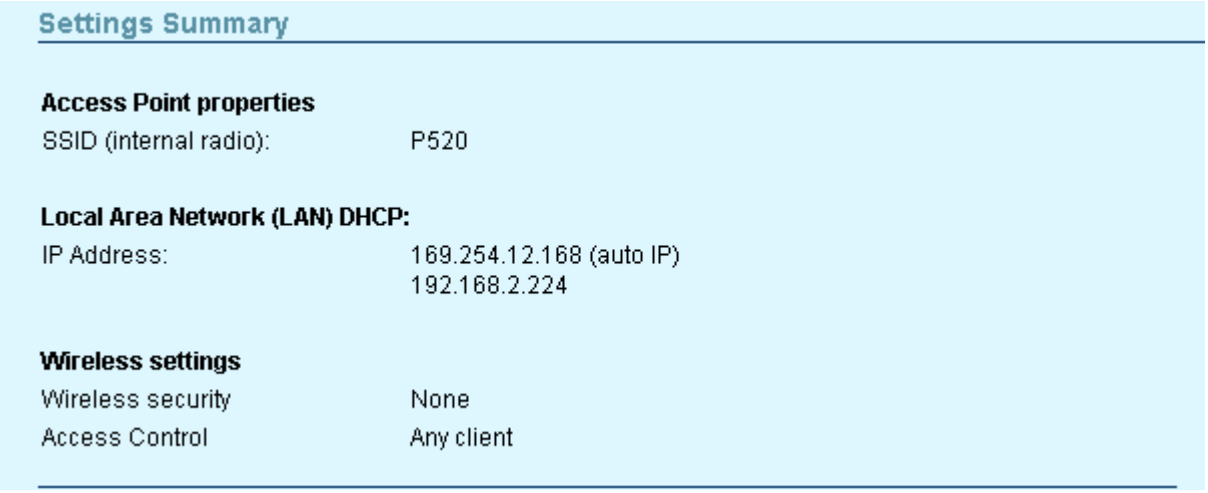


Figure 21 – Settings Summary

SSID – indicates the unique name for your wireless network.

IP Address – indicates the IP address of your P-520.

If two addresses are displayed this means that the access point retrieved its IP address dynamically via DHCP. The first IP address is the IGMP IP multicast address; the second IP is given from DHCP server's pool.

Wireless Security – indicates if security methods are enabled on your access point [None, WEP, WPA, 802.1X].

Access Control – indicates access control status [Any client/Selected clients only].

Configuration | Configuration | Identity

The identity data of the access point are displayed here. You can use the first three fields **Name**, **Location**, **Contact** to describe the access point. These fields do not influence the behavior of the access point. But are for information purposes only.

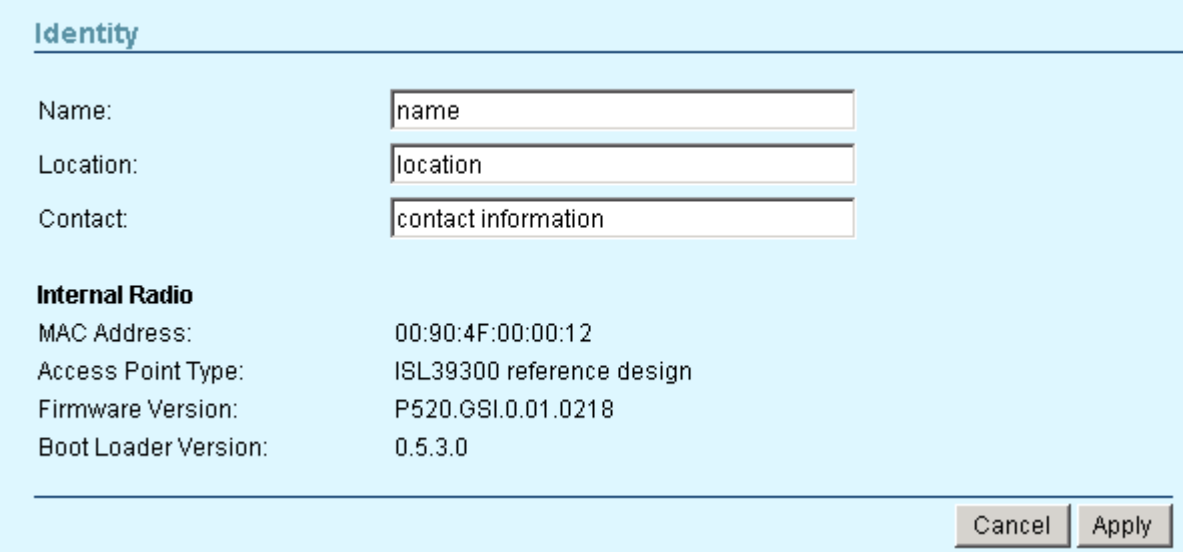


Figure 22 – Identity Settings

Name – specify the administrative name of the access point [string].

Location – specify the location where your device is installed [string].

Contact – specify the name of the person/company responsible for the P-520 [string].

MAC Address – displays the MAC address of the access point. Cannot be changed.

Access Point Type – displays information on your type of access point. Cannot be changed.

Firmware Version – displays the version number of the software that controls the access point.

Boot Loader Version – displays the boot loader version.

Cancel – restore all previous values.

Apply – save changed configuration.

Configuration | Local Area Network | Network Setup

The IP configuration as described below is required for device management purposes. IP addresses can either be retrieved from a DHCP server or configured manually.

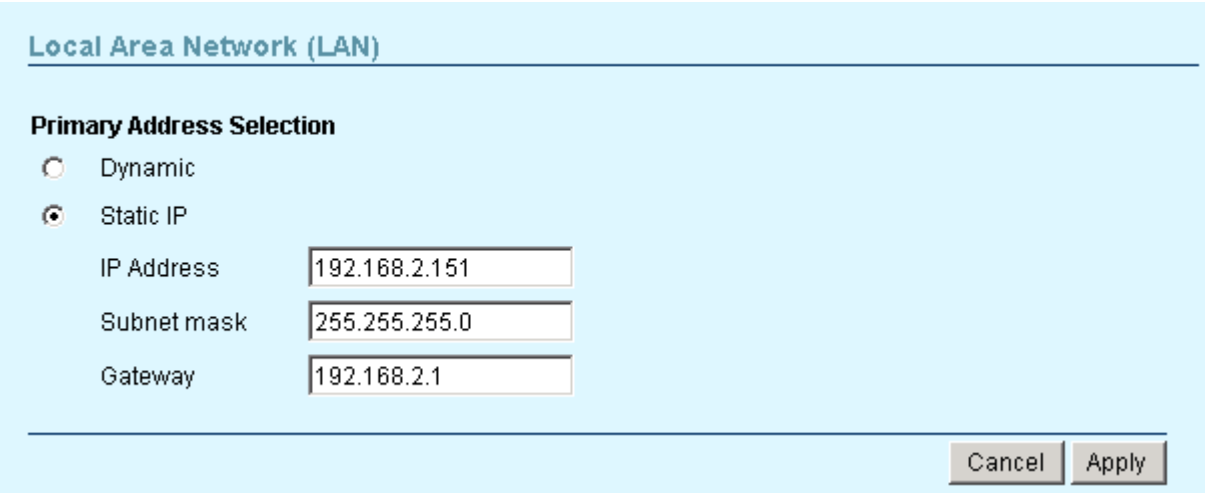


Figure 23 – Network Setup Settings

IP Address – specify the access point's IP address [digit and dots]. When shipped from the factory or reset to factory settings, the AP defaults to a static IP address of 192.168.2.2.

Subnet Mask – specify the access point's subnet mask [digit and dots]. When shipped from the factory or reset to factory settings, the AP defaults to a subnet mask of 255.255.255.0.

Gateway – specify the IP address of the access point's gateway [digit and dots]. When shipped from the factory or reset to factory settings, the AP defaults to a gateway IP address of 192.168.2.1.

If you change the IP address manually, make sure that the chosen IP address is unused and belongs to the same IP subnet as your wired LAN, otherwise you will loose the connection to the P-520 from your current PC. If you enable the DHCP client via a Web browser, the browser will loose the connection after rebooting, because the IP address assigned by the DHCP server is not predictable.

If **Dynamic** is selected the static IP settings are displayed but have no affect on the network configuration. The dynamic IP address and gateway address as assigned by the DHCP server are applied to the system after restart.

To find your P-520 with dynamic IP settings use a utility such as Gemtek Systems **KickStart**.

Configuration | Local Area Network | Virtual LAN

A Virtual Local Area Network (**VLAN**) is a mechanism to segregate devices or groups of devices on the same physical LAN. P-520 allows the definition of a VLAN by a VLAN identifier. If you enable the VLAN functionality in the menu **Configuration | Local Area Network | Virtual LAN** all traffic from the wireless LAN to the LAN will be tagged with the specified VLAN ID. Incoming traffic from the wired LAN not tagged with the appropriate VLAN ID is discarded by the AP.

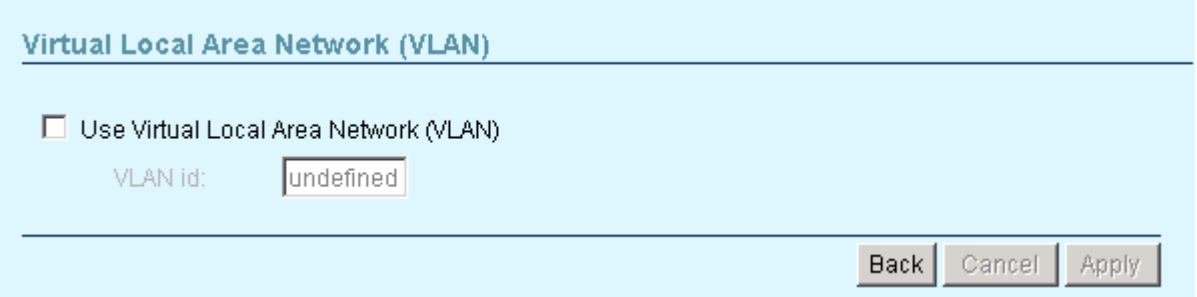


Figure 24 – Virtual Local Area Network (VLAN) Settings

To define a VLAN membership on the access point, select the checkbox and enter the VLAN identifier:

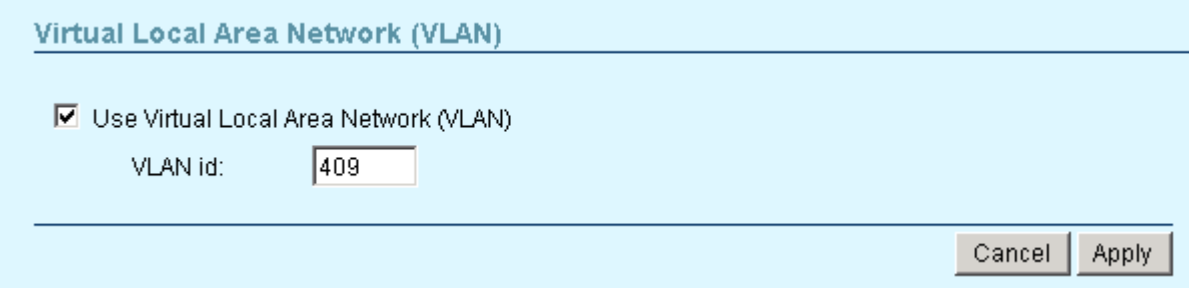


Figure 25 – Enable Virtual Local Area Network (VLAN)

VLAN id – specify the ID for your VLAN network [1 to 4094]. Wireless client devices connected to the AP are grouped into this VLAN.

Cancel – restore all previous values.

Apply – save changed configuration.

When VLAN is enabled you can view this interface statistic in **Status | Interface Statistics** page. There you can see such parameters as interface status, InOctets, InUcast, InMcast, OutOctets, OutUcast and OutMcast.

Configuration | Wireless | Basic Settings

Use the **Configuration | Wireless | Basic Settings** menu to configure the most relevant wireless settings of your access point.

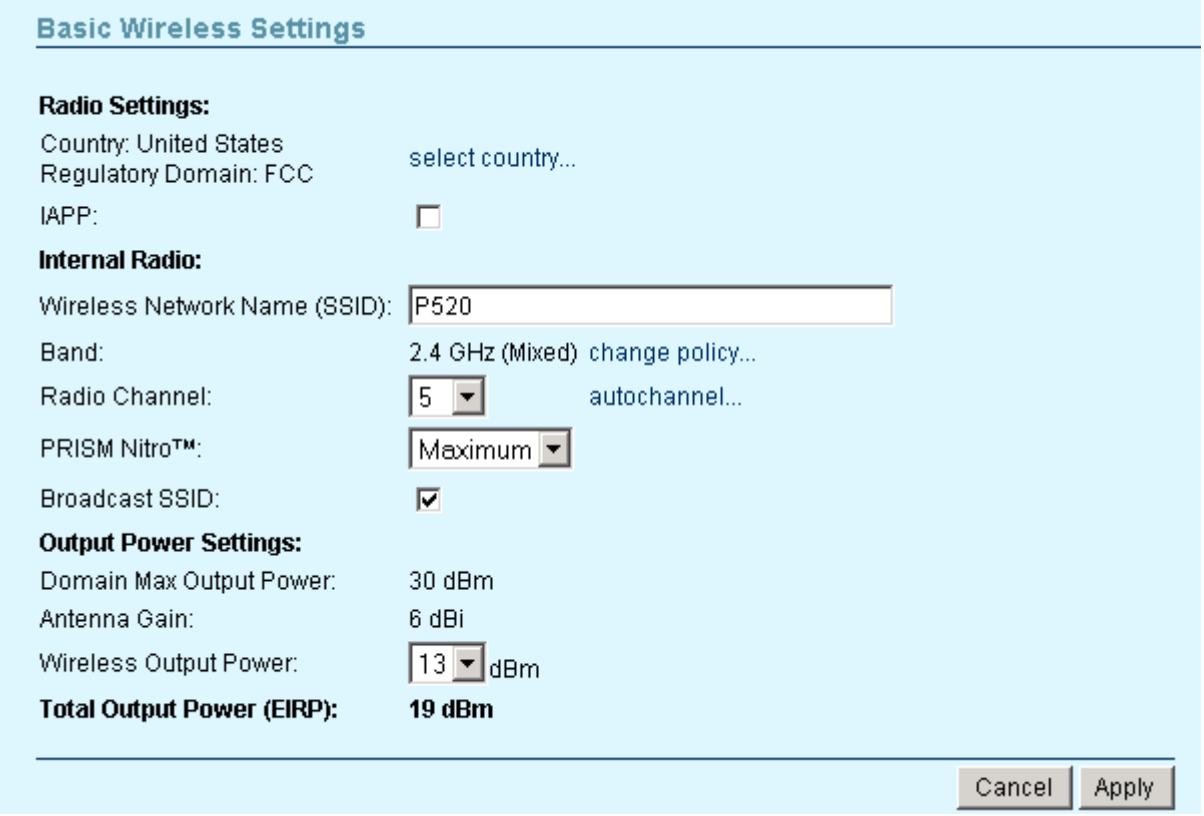


Figure 26 – Basic Wireless Settings

Country – click on the **select country…** link and choose from drop-down list the country in which you will use the AP. According to the country chosen the regulatory domain settings change. You are not allowed to select radio channels and RF output power values other the permitted values for your country and regulatory domain. See also appendix **B) Regulatory Domain/Channels**.

Regulatory Domain – displays the regulatory domain according selected country [ETSI/FCC]. Not configurable.

IAPP – select this checkbox to enable seamless roaming of client stations between P-520 APs.

By using the Inter-Access Point Protocol (IAPP) roaming, a client can be hand-over between access points when changing its physical location. The IAPP protocol is used to ensure all relevant session information is delivered to the new AP to which the client is moving. IAPP roaming is compatible with other Gemtek Systems products.

Look at the scheme for more details about IAPP roaming:

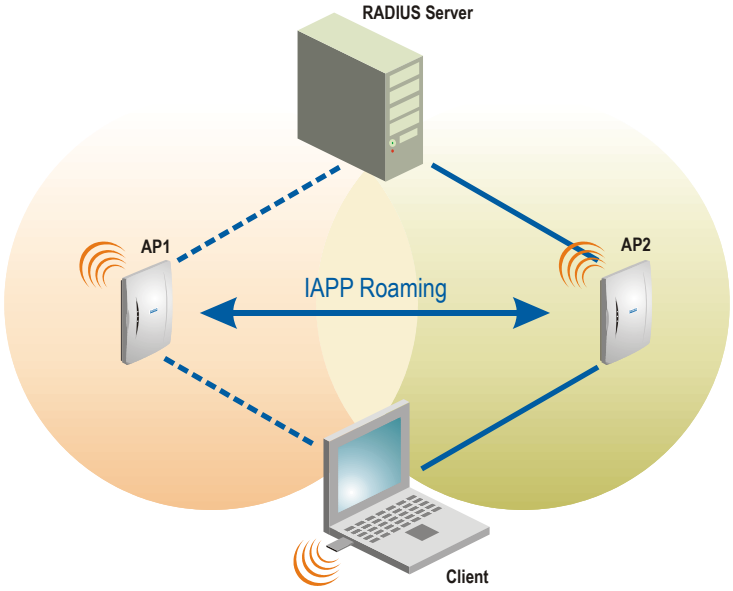


Figure 27 – IAPP Roaming Scheme

The wireless client is switched from AP1 to AP2 when entering the coverage area of the new access point (AP2). The roaming is performed without client re-authentication. The IAPP protocol ensures to inform the old AP1 of the new client association. The AP1 then stops the client RADIUS session, and the AP2 starts the client's session with the RADIUS.

IAPP roaming requires that all access points share the same SSID.

Wireless Network Name (SSID) – is a unique name for your wireless network [1-32 symbols]. The default SSID is "P520" but you should change this to a personal wireless network name. The SSID is important for client stations when connecting to the access point. All client stations must have their client SSID settings configured and must use the same SSID.

Band – click on the **change policy…** link and choose the policy of internal radio mode [Mixed/G-only/B-only].

Changing the radio policy could result in a loss of your connection when you are using a wireless connection.

Radio Channel – select the channel that the access point uses to transmit and receive information. Multiple frequency channels are used to avoid interference between nearby access points. If you wish to operate more than one access point in overlapping coverage areas, we recommend a distance of at least four channels between the chosen channels. For example, for three access points in close proximity choose channels 1, 6 and 11.

Before changing radio settings manually, verify that these settings comply with your national regulations. At all times, it is the responsibility of the end-user to ensure that the installation complies with local radio regulations. Refer to the appendix, **B) Regulatory Domain/Channels** for more details.

Click on the **autochannel…** link and a pop-up window with auto channel settings will appear. You can now select a list of preferred channels:

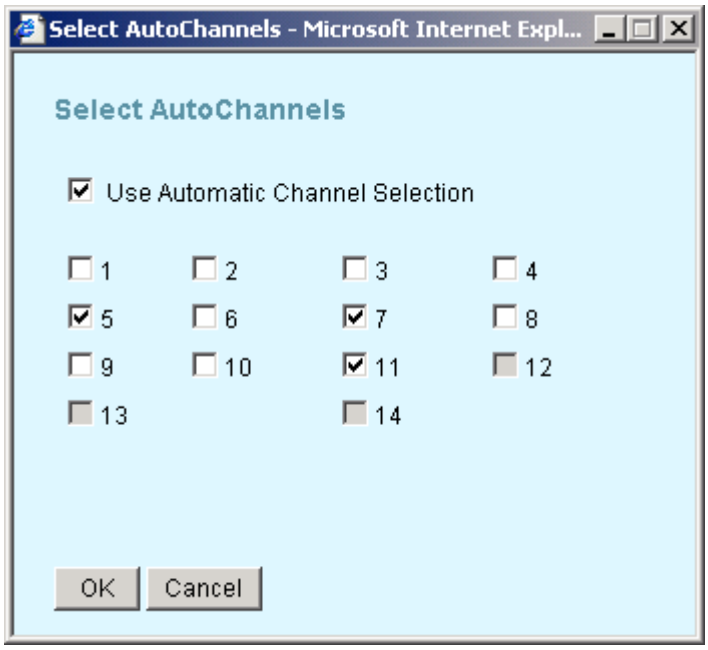


Figure 28 – Auto Channel Settings

The **auto-channel** function is a great technique to minimize interference between access points. With auto-channel selection enabled the P-520 will regularly scan the air for neighboring access points and selects the channel with the least expected interference. The range of scanned channels can be limited by the administrator.

Do not use auto-channels when using WDS, otherwise the access points will not be able to communicate between each other wirelessly.

PRISM Nitro™ – increases the performance in 802.11g and mixed-mode environments. The Nitro technology provides up to 50% more throughput in g-only networks; up to 300% more in mixed-mode (802.11b and 802.11g) networks by eliminating collisions and employing packet bursting technology. A maximum of 140Mbps throughput can be reached by selecting a packet burst lengths of 1500μs:

- **Off** – switch off PRISM Nitro™,
- **Minimum** – burst length is 650 μs,
- **Medium** – burst length is 1000 μs,
- **Maximum** – burst length is 1500 μs;

Broadcast SSID – when selected your AP's SSID is visible during network scans on a wireless station. When unselected, the AP's SSID is not visible and not broadcasted to wireless stations.

Domain Max Output Power – indicates the maximal output power according selected regulatory domain. Cannot be modified.

Antenna Gain – is the gain of the connected antenna in relation to an isotropic radiated power (dBi). Cannot be modified.

Wireless Card Output Power – select the wireless card output power in dBm. Wireless card output power list will vary according selected regulatory domain.

Total Output Power (EIRP) – is the maximum radiated output power of the antenna (strength of the radio signal transmitted). Cannot be modified. It is also referred to as the maximum **EIRP** (Effective Isotropic Radiated Power) value (dBm). The higher is the number, the stronger the signal is.

Cancel – restore all previous values.

Apply – save changed configuration.

Configuration | Wireless | WDS Links

The access point P-520 supports the definition of a WDS (Wireless Distribution System). In WDS mode a P-520 can act as wireless bridge or wireless repeater. Choose the **Configuration | Wireless | WDS Links** menu if you want to setup bridge links between different access points while connecting wireless client stations in parallel. Up to seven access points can be interconnected in a wireless distribution system.

In the WDS table bride links can be defined by selecting WDS ready access points by their MAC address. Make sure that the **radio channel** and the **data rates** for all WDS APs **are set to the same values**.

APs that relay data received from a wireless station to another access points (and vice versa) have to receive and send each packet over the same channel. Hence the overall throughput will be reduced for each relay link.

As an option WDS links to other APs can be added manually by specifying the MAC address of the remote AP.

APs participating in a WDS network **DO NOT** have to be configured with the **same SSID**.

Add AP in WDS from the WDS Links table:

In the menu Configuration | Wireless | WDS Links you can find a table of remote access points that you can connect to via a WDS Link. On this table an administrator can see access points, their operating channels, data rates, RSSI (Received Signal Strength Indication) and the Age of the last signal.

Select the checkbox to add an access point to the Wireless Distribution System. The checkboxes will be active only of those WDS links that uses the same channel as your device:

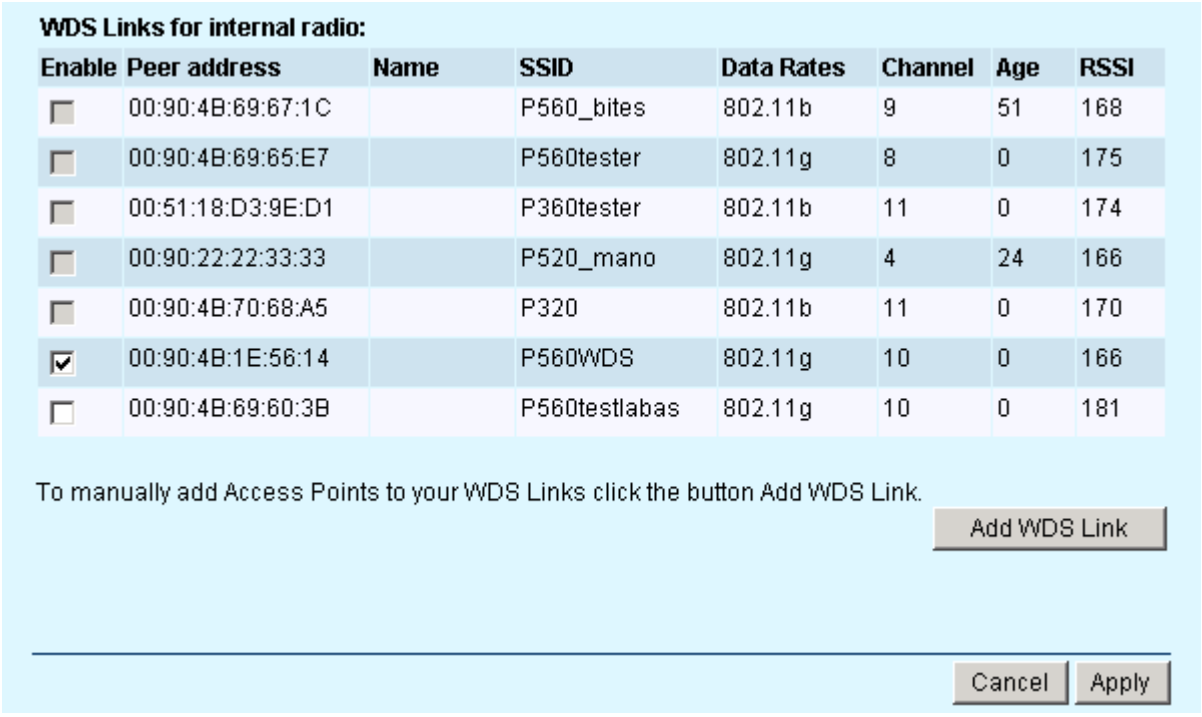


Figure 29 – WDS Links for Internal Radio Table

Enable – select if need to add the access point to Wireless Distribution System.

Peer address – displays the MAC address of the access point.

Name – specify the name of chosen WDS Link.

SSID – displays the SSID of the access point.

Data Rates – displays the transmit data rates of the remote access point.

Channel – displays the channel that the access point uses to transmit and receive information.

Age –indicates the age of the last information received from the remote access point in seconds.

RSSI – shows the Received Signal Strength Indication (RSSI) of the access point.

Cancel – restore all previous values.

Apply – save changed configuration.

When the required WDS Link is selected, enter the name of chosen WDS Link:

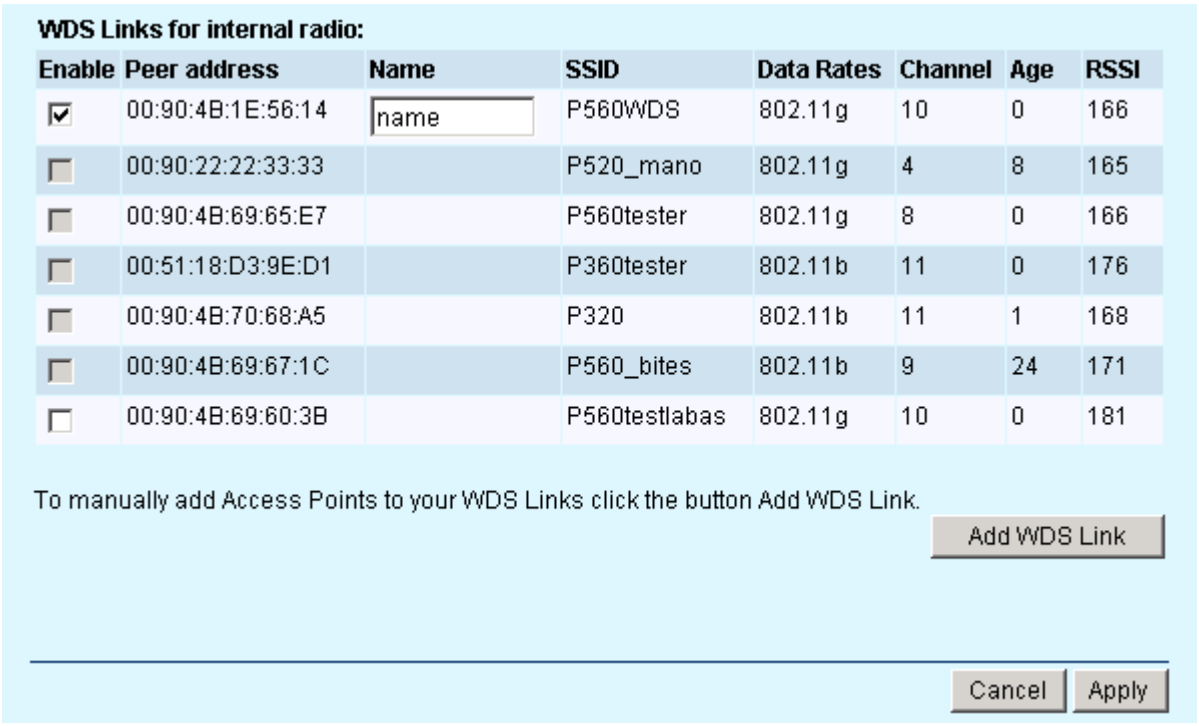


Figure 30 – Specify the WDS Link Name

Cancel – restore all previous values.

Apply – save changed configuration.

Add AP in WDS manually:

When a WDS APs is not shown in the WDS table automatically you can add it manually by entering the MAC address of the remote AP. Click on the **Add WDS Link** button.

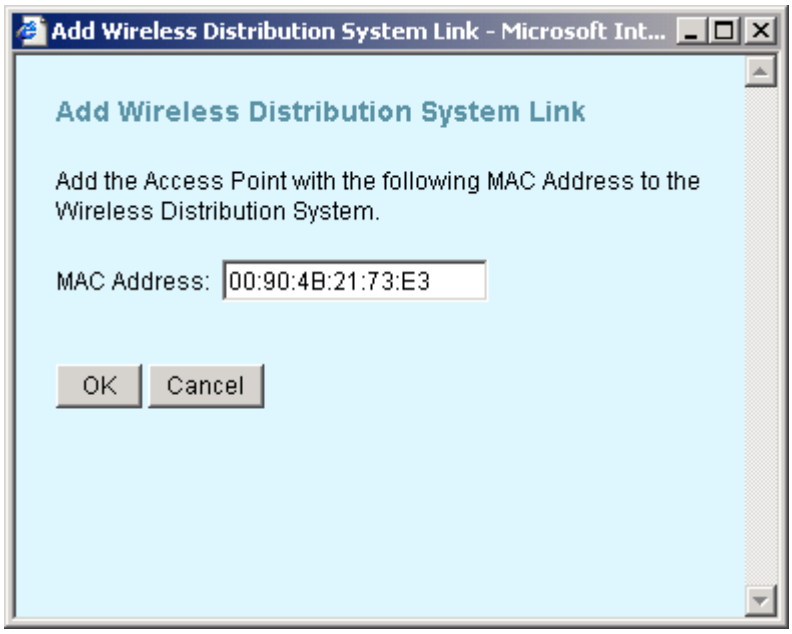


Figure 31 – Add WDS Link Manually

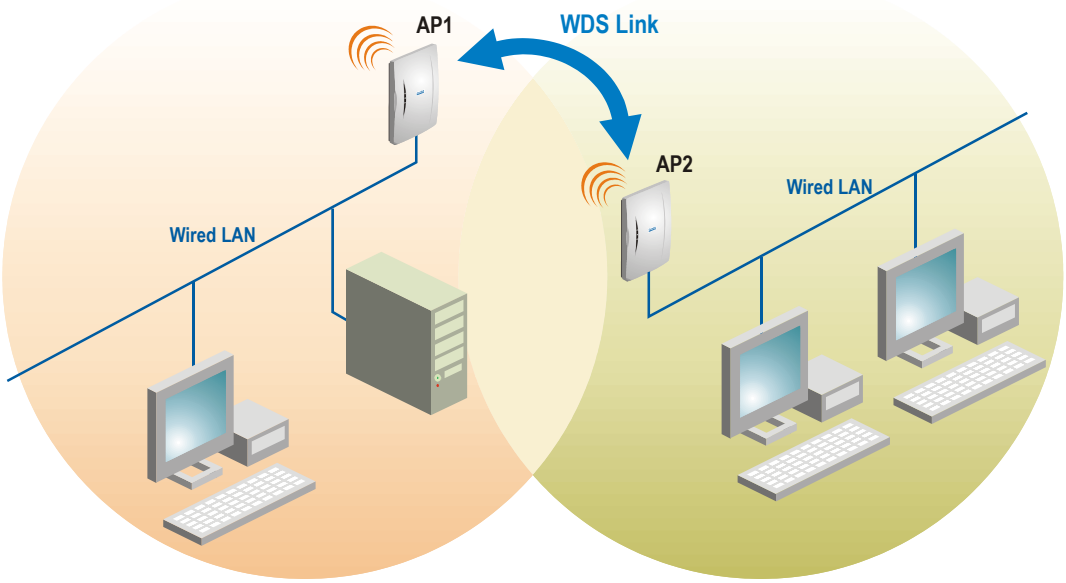
OK – saves added new WDS Link in the **WDS Links for internal radio** table.

Cancel – close the **Add Wireless Distribution Link** window without saving information.

Follow the example to see how to configure a WDS.

Case 1 – AP with WDS (Wireless Bridge).

Create the wireless bridge between two wired networks: AP1 can be configured to forward all data to AP2 and vice versa.



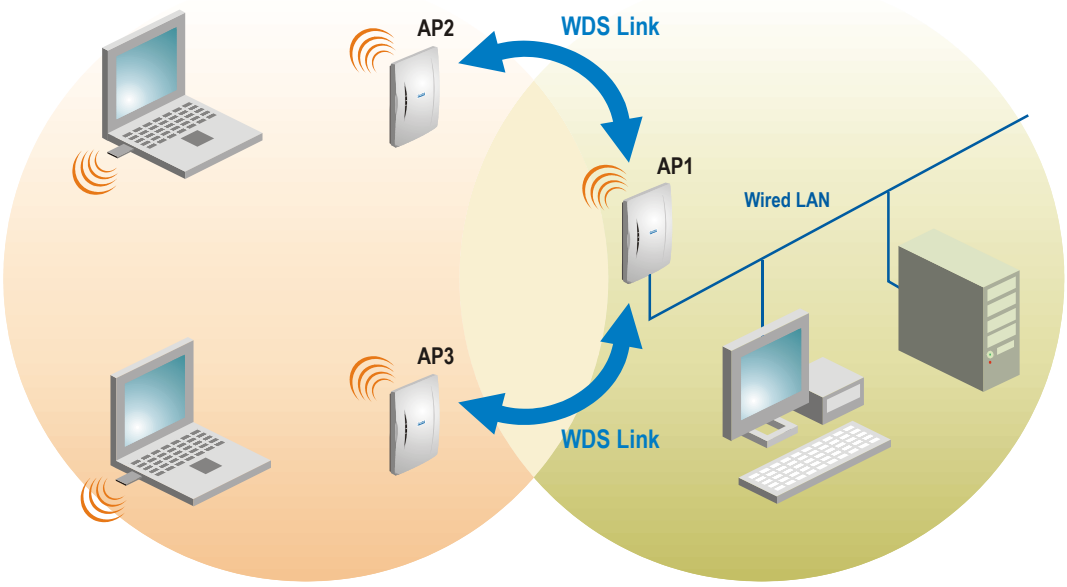
Step 1 Choose the **wireless MAC** address of **AP2** in the web configuration interface of **AP1**, menu **WDS Links**.

Step 2 Choose the **wireless MAC** address of **AP1** in the web configuration interface of **AP2**, menu **WDS Links**.

Step 3 Select the **same radio channel** and the **data rates** for both APs using the **Wireless Settings** menu.

Case 2 – AP with WDS (Wireless Repeater)

This example shows a configuration where one AP relays all traffic wirelessly to another AP. In the picture below Station 1 is connected to the wired LAN via AP1 and AP2. AP 1 acts as a repeater between Station 1 and AP2.



Step 1 Choose the **wireless MAC** address **AP2 and AP3** in the **AP1** Web interface **WDS Links** menu under the **Configuration**.

Step 2 Choose the **wireless MAC** address **AP1** in the **AP2** Web interface **WDS Links** menu under the **Configuration**.

Step 3 Choose the **wireless MAC** address **AP1** in the **AP3** Web interface **WDS Links** menu under the **Configuration**.

Step 4 Select the **same radio channel** for both APs using the **Wireless Settings** menu under the **Configuration**.

Configuration | Wireless | Advanced Settings

For normal operation the following default settings do not need to be modified. Changing the P-520 advanced settings requires expert knowledge of the 802.11 protocol and the radio functionality.

The configuration menu **Configuration | Wireless | Advanced Settings** allows administrators to change low level radio parameters:

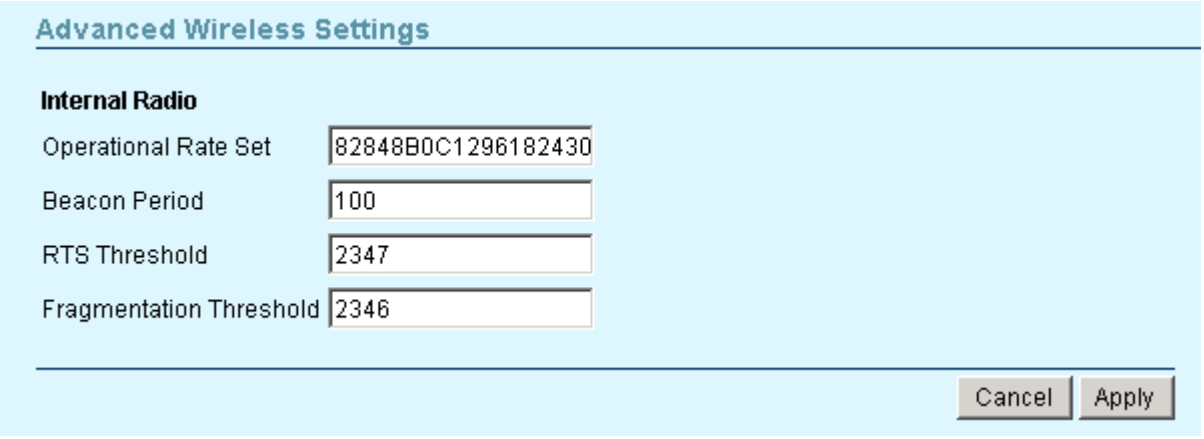


Figure 32 – Advanced Wireless Settings

Operational Rate Set – this setting specifies the set of Supported and Basic data rates at which the station may transmit data. Each rate shall be within the range from 2 to 127, corresponding to data rates in increments of 500 kb/s from 1 Mb/s to 63.5 Mb/s, and shall be supported for receiving data. This value is reported in transmitted Beacon, Probe Request, Probe Response, Association Request, Association Response, Reassociation Request, and Reassociation Response frames, and is used to determine whether a BSS with which the station desires to synchronize is suitable.

Operational rate set is defined as hexadecimal string where highest bit of each digit represents if Supported rate is the Basic rate (basic rate = supported rate | 0x80, where "|" means "bitwise or" operation).

Beacon Period – this setting specifies the amount of time between beacons in milliseconds. A beacon is a packet broadcast by the access point to synchronize the wireless network.

RTS Threshold – this setting specifies the maximum packet size beyond which the Wireless LAN Card invokes its RTS/CTS mechanism. Packets that exceed the specified RTS threshold trigger the RTS/CTS mechanism. The NIC transmits packets smaller than this threshold without using RTS/CTS [[0-2347] default: 2347 (2347 means that RTS is disabled)].

Fragmentation Threshold – the fragmentation threshold, specified in bytes, determines whether packets will be fragmented and at what size. On an 802.11 wireless LAN, packets exceeding the fragmentation threshold are fragmented, i.e., split into, smaller units suitable for the circuit size. Packets smaller than the specified fragmentation threshold value are not fragmented [[256-2346] default: 2346 (2346 means that fragmentation is disabled)].

Cancel – to restore all previous values.

Apply – to save changed configuration.

Configuration | Security | Wireless Security | Client Isolation

Use the **Configuration | Security | Wireless Security| Client Isolation** menu to configure the layer 2 user isolation feature. Select the **Use Client Isolation** checkbox to enable Layer 2 wireless client separation. In this case connected wireless stations are not able to communicate with each other. The client stations are isolated on MAC address level.

Figure 33 – Client Isolation Settings

Back – to return to the main **Wireless Security Settings** page.

Cancel – to restore all previous values.

Apply – to save changed configuration.

Configuration | Security | Wireless Security | Access Control List

In the **Access Control Settings** page (**Access Control List (ACL)** menu under the **Configuration | Security | Wireless Security**) you can specify default access policy for the Wireless device interface or define special access rules. To enable Access Control List select the **Enable access control list** checkbox.

Default Access: select **Accept** to allow all mobile clients to access this access point or **Reject** to prevent all mobile clients from accessing your access point. Clients may also be subject to rules in the Access control table.

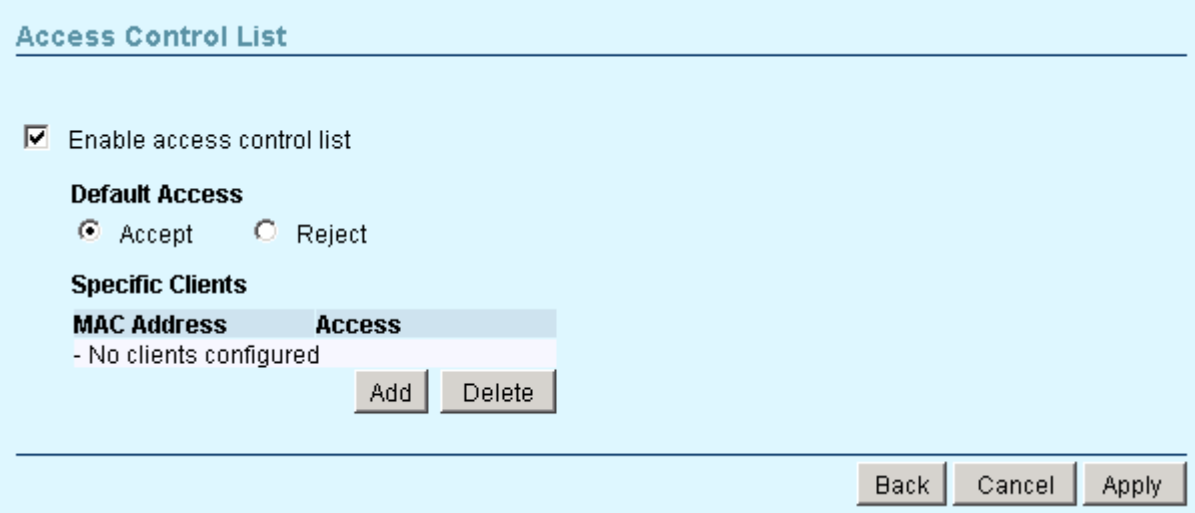


Figure 34 – Access Control List (ACL) Settings

You can further create your own access list if you need to define special access rules for specific network devices. The access control list is based on the network device's MAC address. In the access control table, you need only specify the network device MAC address and its access policy (accept/reject) with the new rule.

Add – click to add ACL rule.

Delete – click to remove selected ACL rule.

Back – to return to the main **Wireless Security Settings** page.

Cancel – to restore all previous values.

Apply – to save changed configuration.

Click the **Add** button to add new ACL rule and new pop-up window **Add a Client** appears. The definition of new rules is shown in the following example:

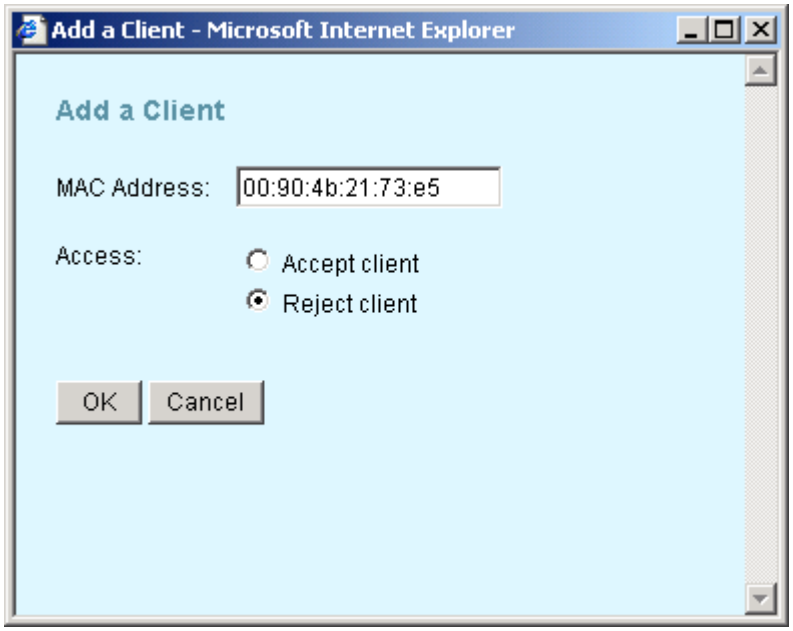


Figure 35 – Add New ACL Rule

MAC Address – specify the MAC address of the device you want to add to the ACL. The format is a list of colon separated hexadecimal numbers (for example: 00:00:78:0A:CD:FF).

Access – select the permission of the rule to determine whether the specified network device shall be accepted or rejected by the access point.

OK – saves added new ACL rule into configuration.

Cancel – close the **Add a Client** window without saving information.

Click the **Delete** button to remove desired ACL rule, and new pop-up window **Delete Clients** appears. You can select the MAC addresses that should be deleted as shown on the following example:

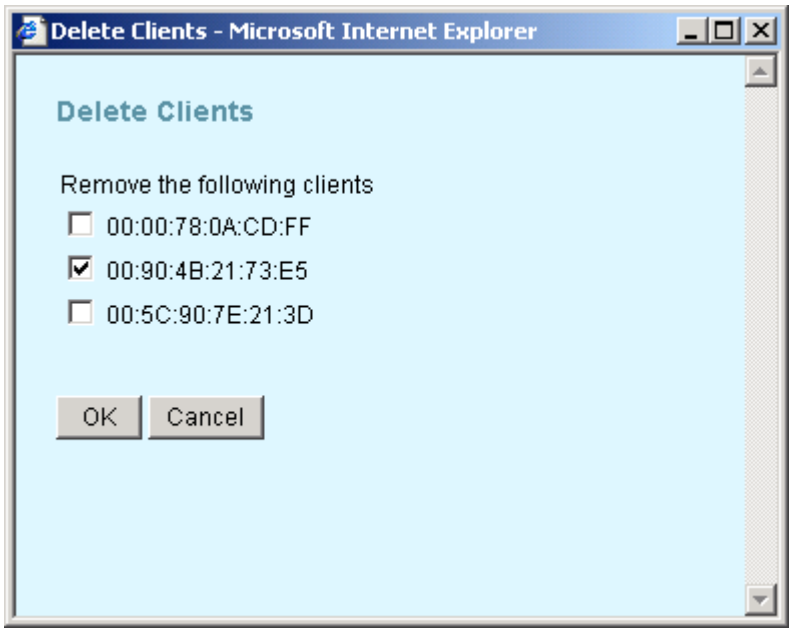


Figure 36 – Delete Selected Clients' MAC addresses

OK – removes selected ACL rule from the list.

Cancel – close the **Delete Clients** window without saving information.

Configuration | Security | Wireless Security | RADIUS Servers

Only 2 RADIUS servers can be configured on the system: one Authentication and one Accounting.

RADIUS is an authentication, authorization and accounting (AAA) system. **RADIUS** enables operators to maintain a very large database of users. By using **RADIUS,** operators can implement policy-based management of their subscriber base. **RADIUS** further enables the collection of usage data (e.g. amount of time, amount of transferred bytes, and session time) for accounting purposes.

Use the **Configuration | Security | Wireless Security| RADIUS Servers** menu to configure the RADIUS servers' list and settings. By default there is no RADIUS server on the system:

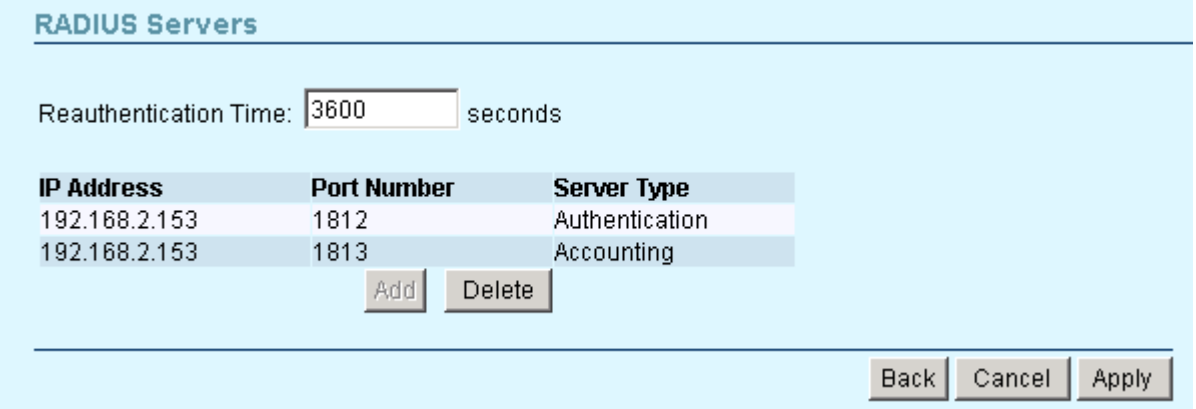


Figure 37 – RADIUS Servers' Settings

Re-authentication Time – specify the number of seconds after which the access point re-authenticates client stations [0-2147483647]. The default value is 3600 seconds. If 0 is entered it means that stations will not have to re-authenticate as long as they are connected.

IP address – displays RADIUS server's IP address.

Port Number – displays RADIUS server's port number.

Type – displays RADIUS server's type.

Add – click to add RADIUS server.

Delete – click to remove selected RADIUS server.

Back – to return to the main **Wireless Security Settings** page.

Cancel – to restore all previous values.

Apply – to save changed configuration.

In the default configuration no RADIUS servers are define on the system. Click the **Add** button to add new RADIUS server and new pop-up window **Add RADIUS server** appears. You can define the RADIUS server's parameters as shown on the following example:

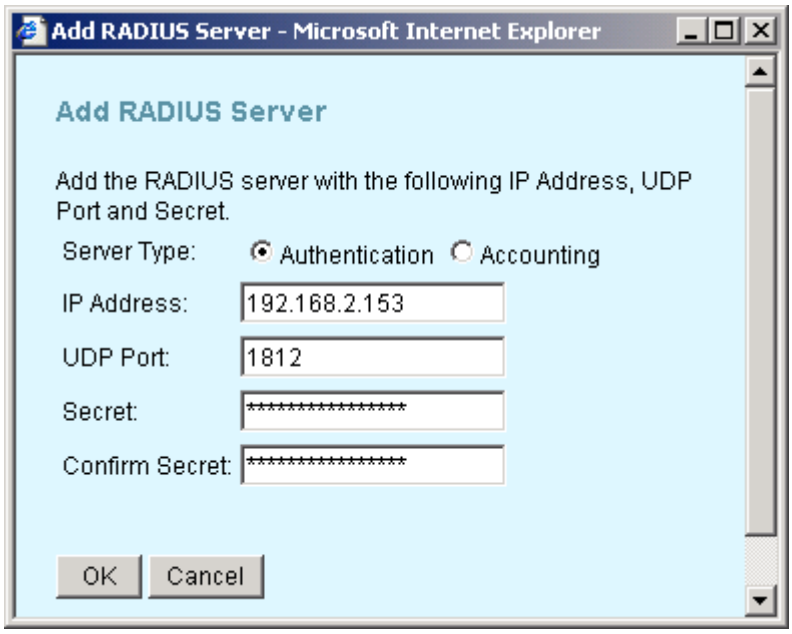


Figure 38 – Add RADIUS Server

Server Type – select the RADIUS server's type [authentication/accounting].

IP Address – enter the RADIUS server IP address [digit and dots].

UDP Port – specify the network port used to communicate with RADIUS [1-65535]. Default: 1812.

The port default value is 1812 in accordance with RFC 2865 " Remote Authentication Dial-in User Service (RADIUS)".

Secret – specify the shared secret string that is used to encrypt data frames used for RADIUS servers [4-64 symbols].

Confirm Secret – re-enter the RADIUS secret to verify its accuracy.

OK – saves added new RADIUS server into configuration.

Cancel – close the window without saving information.

Click the **Delete** button to delete desired RADIUS server, and new pop-up window **Delete RADIUS Servers** appears. You can select the RADIUS server that should be deleted as shown on the following example:

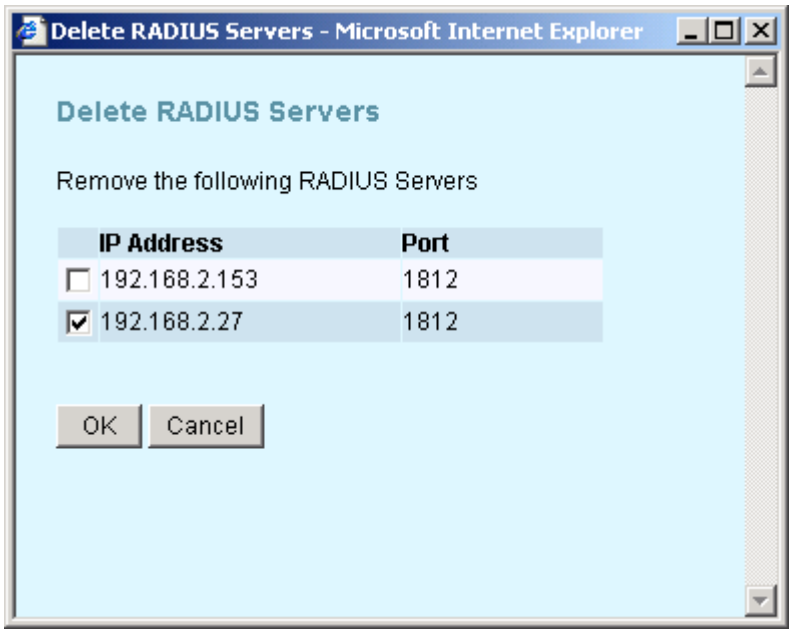


Figure 39 – Delete RADIUS server

OK – removes selected RADIUS servers from the system.

Cancel – close the window without saving information.

Configuration | Security | Wireless Security | Wired Equivalent Privacy (WEP)

WEP is a data privacy mechanism based on a 64-bit or 128-bit shared key algorithm as described in the IEEE 802.11 standard. Static WEP uses a symmetric scheme where the same key and algorithm are used for both encryption and decryption of data.

Use the **Configuration | Security | Wireless Security| Wired Equivalent Privacy (WEP)** menu to configure the WEP encryption.

The checkbox **Use WEP Encryption** defines if encryption will be used or not. To enable WEP encryption, select this checkbox:

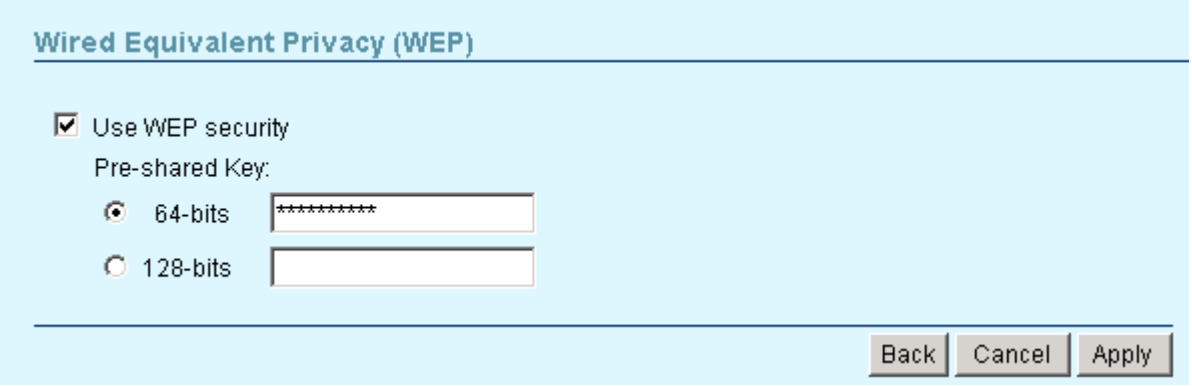


Figure 40 – Wired Equivalent Privacy (WEP) Settings

Enter the encryption key to be used to encrypt and decrypt wireless traffic:

64-bits – specify pre-shared key as 5 colon-separated HEX (0-9, A-F, and a-f) pairs (e.g. 00:AC:01:35:FF).

128-bits – specify pre-shared key as 13 colon-separated HEX (0-9, A-F, and a-f) pairs (e.g. 00:11:22:33:44:55:66:77:88:99:AA:BB:CC).

Back – return to the main **Wireless Security Settings** page.

Cancel – restore all previous values.

Apply – save changed configuration.

The same encryption key must also be entered into the WLAN card configuration of the mobile clients.

Configuration | Security | Wireless Security | 802.1x Security

802.1X security is available only if RADIUS server is configured on the P-520 system.

Use the **Configuration | Security | Wireless Security| 802.1x Security** menu to setup the 802.1X security settings. This security always uses dynamic WEP keys which length you can choose by simply selecting the radio button.

To enable 802.1x security, select the checkbox and choose the desired Key Size and settings for Rekeying:

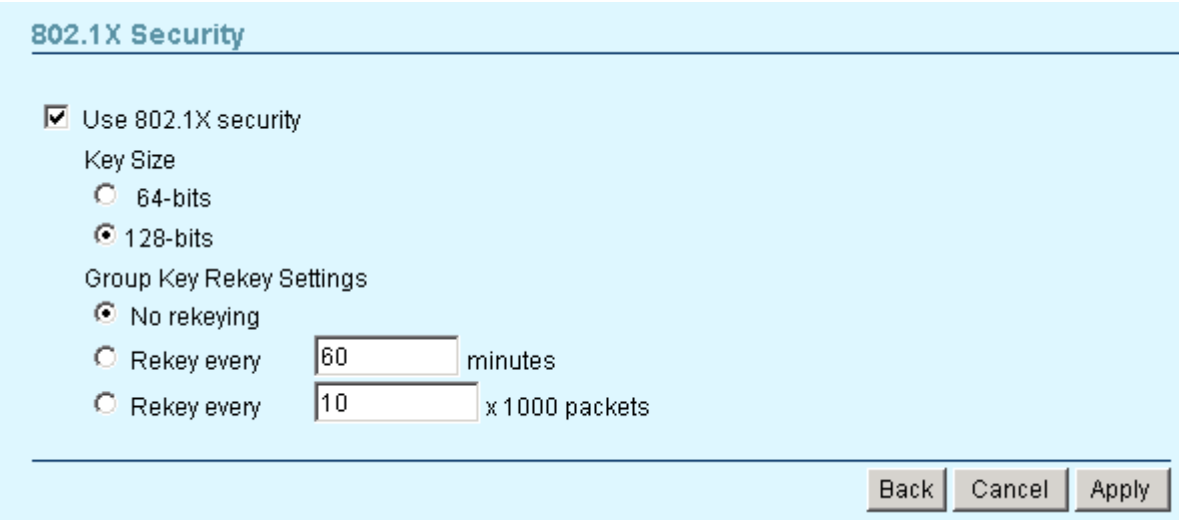


Figure 41 – 802.1X Security Settings

Key Size and Group Rekeying unavailable when using WEP security.

64-bits – indicates that a 64-bit key is chosen for 802.1x security.

128-bits – indicates that a 128-bit key is chosen for 802.1x security.

No rekeying – indicates that Group Key will not be changed dynamically.

Rekey every … minutes – specify the time period in minutes, after which the group key will be updated [1-71582788]. Default value is 60 minutes.

Rekey every … x1000 packets – specify the number of transmitted packets, per 1000 packets, after which the group key value will be updated [1-4294967295]. Default value is 10x1000 packets.

Configuration | Security | Wireless Security | Wi-Fi Protected Access (WPA)

Wi-Fi Protected Access provides a higher level of protection for wireless LAN client stations as it includes methods for mutual authentication, strong encryption, and data integrity. WPA takes the original master key only as a starting point and derives its encryption keys dynamically from this master key. WPA regularly changes and rotates the encryption keys so that the same encryption key is never used twice. Key exchange is done automatically transparent to the user.

To enable the WPA security for your WLAN you need:

- An access point that has WPA support like the Gemtek Systems P-520
- A wireless network card with WPA ready driver
- A supplicant that supports WPA (e.g. Windows XP client)

To configure the WPA with pre-shared key security on the P-520 use the **Configuration | Security | Wireless Security| Wi-Fi Protected Access (WPA)** menu, select the WPA with pre-shared key security method and enter the shared secret:

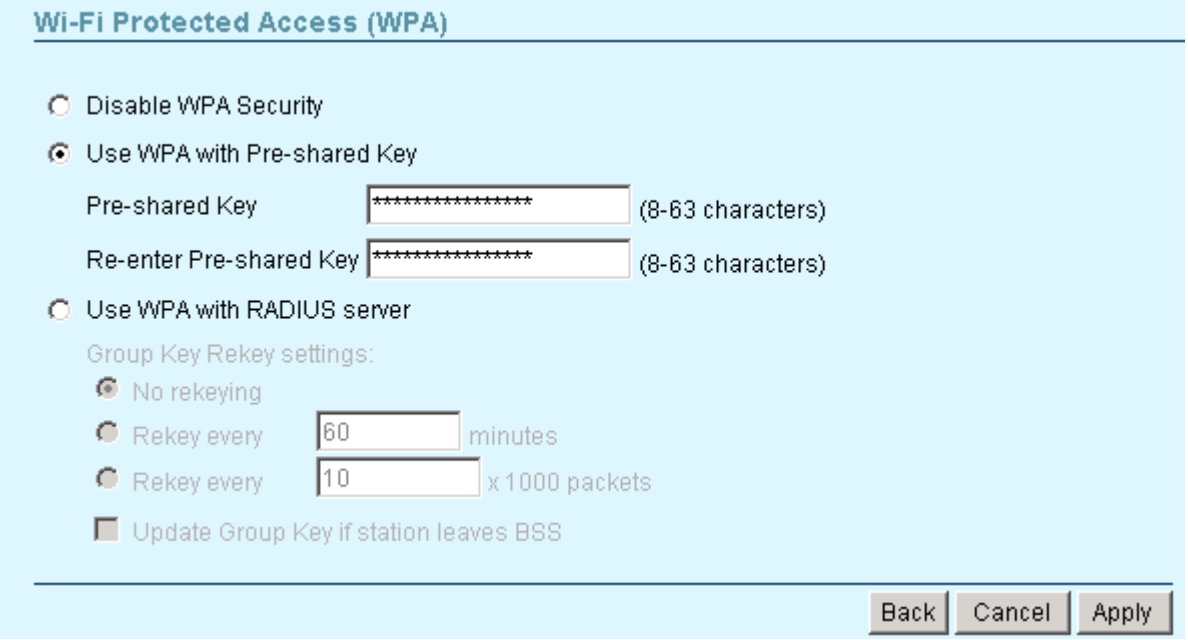


Figure 42 – WPA with Pre-shared Key Settings

Pre-shared Key – specify the pre-shared key for WPA security [8-63 characters].

Re-enter Pre-shared Key – re-enter pre-shared key to verify its accuracy.

The pre-shared key must match the one configured on your WLAN client stations.

Back – return to the main **Wireless Security Settings** page.

Cancel – restore all previous values.

Apply – save changed configuration.

WPA with RADIUS server makes use of external AAA (RADIUS) server to generate and exchange dynamic WPA keys between P-520 and the client stations. To configure WPA with a RADIUS server select the **WPA with RADIUS server** security method radio button and enter the Group Key Rekey settings:

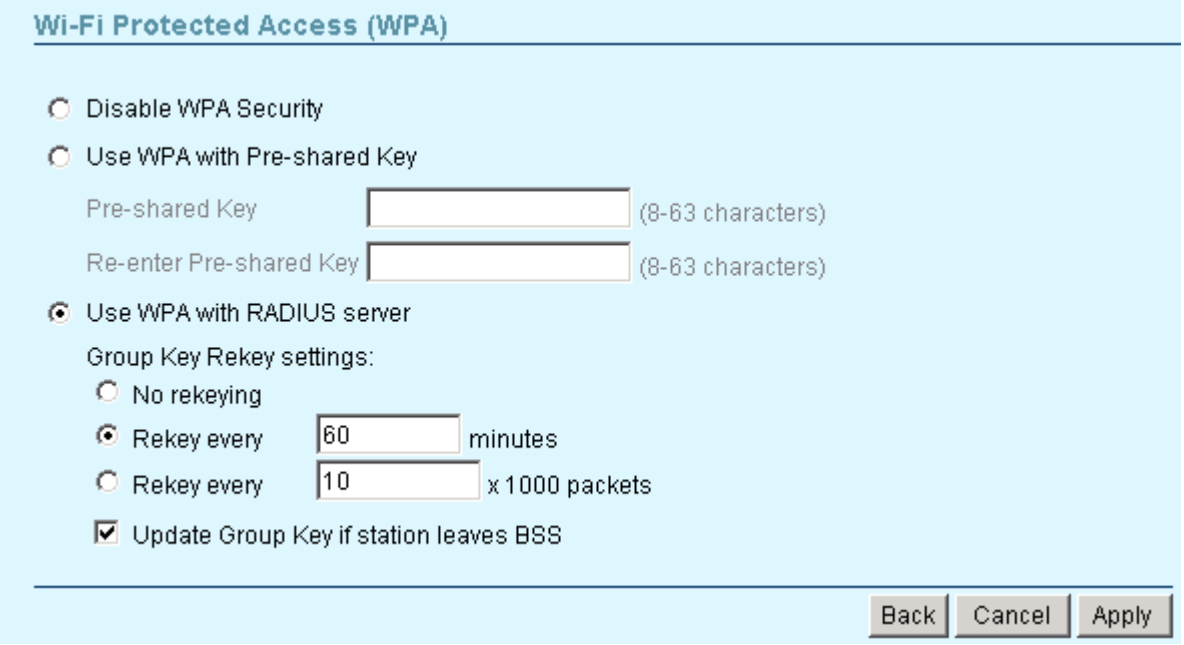


Figure 43 – WPA with RADIUS Server Settings

No rekeying – indicates that Group Key will not be rekeyed.

Rekey every … minutes – specify amount of minutes and WPA automatically will generate a new

Rekey every … minutes – specify the time period in minutes, after which the group key will be updated [1-71582788]. Default value is 60 minutes.

Rekey every … x1000 packets – specify the number of transmitted packets, per 1000 packets, after which the group key value will be updated [1-4294967295]. Default value is 10x1000 packets.

Update Group Key if station leaves BSS – when selected, the group key value will be updated if wireless client leaves BSS.

Configuration | Security | Wireless Security | Management Security

Use the **Configuration | Security | Wireless Security** | **Management Security** menu for changing the administrator's password and to lock the access point for any further configuration changes.

The default administrator settings for all access point interfaces are:

username - **admin**
password - **admin01**

The username is not configurable parameter, so it cannot be changed.

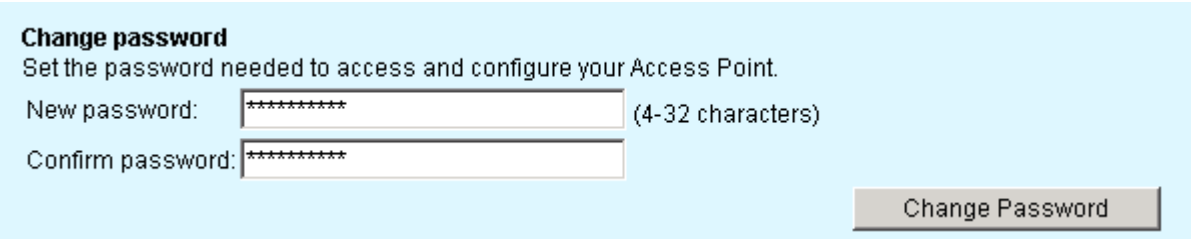


Figure 44 – Change Administrator's Password

New Password – specify new password value used for user authentication in the system [4-32 characters].

Confirm Password – re-enter the new password to verify its accuracy.

Change Password – changes new specified administrator's password.

The password is also the SNMP Read-write community string. If the password is changed the SNMP community string will be changed as well.

Use **Lock Access Point** to prevent modifications to the current device configuration.

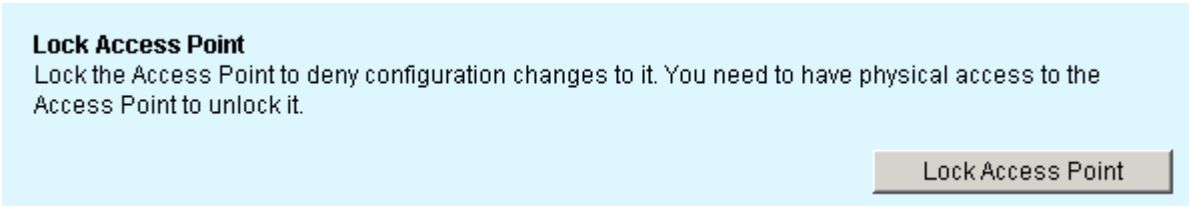


Figure 45 – Lock Access Point

Lock Access Point – click the button to lock the P-520.

This action denies system configuration modifying. You will not be able to configure any of device settings. To unlock the access point you need the physical access to the P-520 and press the **reset** button on the device for 1 second.

Keep in mind that **reset** button will set the administrator password back to default:
User Name: **admin**
Password: **admin01**

Configuration | System | Backup/Restore

To restore s saved system configuration, set factory defaults or download current system configuration use the **Backup/Restore** menu.

Restore Configuration allows you to upload a backup configuration from disk to the P-520. Simply select the configuration file from disk and click **upload**:

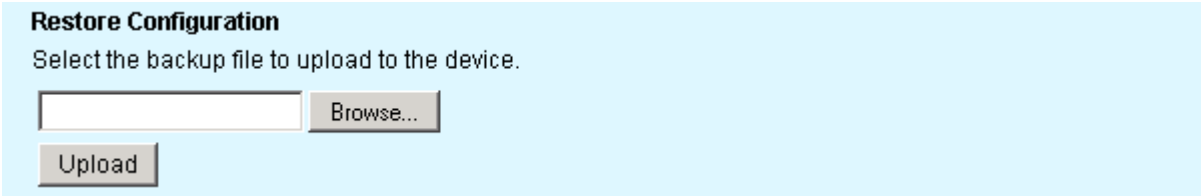


Figure 46 – Upload System Configuration File

Browse – specify file you want to upload location.

Upload – upload system configuration on the system.

Backup Configuration allows you to download the current system configuration and save to a file. Simply click the **Backup** button and specify the file location and name.

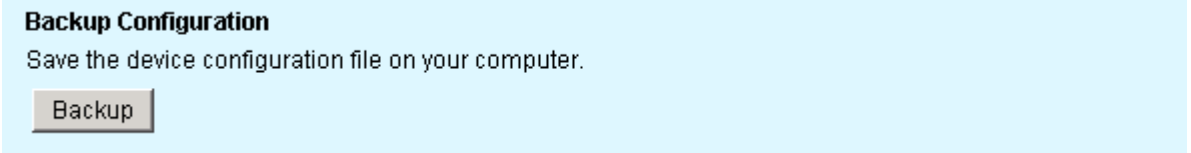


Figure 47 – Download System Configuration File

Backup – save the configuration as a file on your computer.

Restore Default Configuration sets the device back to its original or default configuration

Check the Factory defaults values in the Appendix section**: C) Factory Defaults Values for the P-520 Access Point**

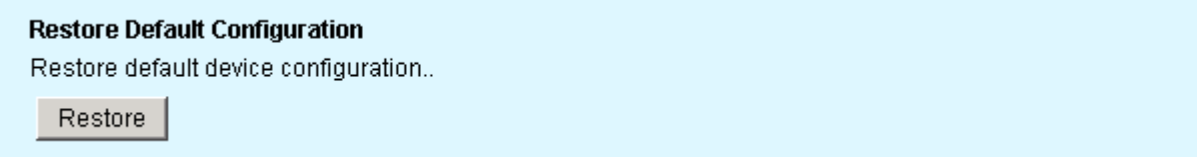


Figure 48 – Restore Default Configuration

Restore – reset device to factory default values.

Keep in mind that resetting the device is an irreversible process.
Please note that also the administrator password will be set back to the factory default.

Reboot. Click this button to reboot the access point:

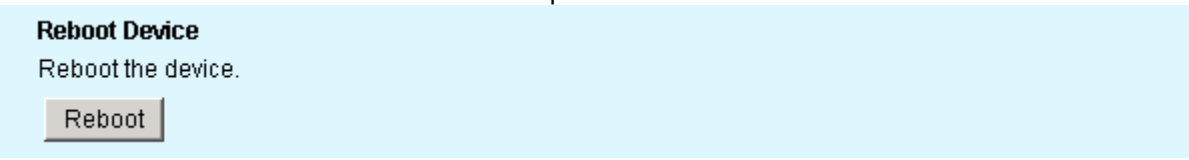


Figure 49 – Reboot the Access Point

Configuration | System | SNMP Traps

SNMP is another management interface for the P-520. In particular it provides the ability to send trap messages with notifications or alarms to a management system. You can configure the SNMP agent in P-520 to send SNMP traps to one or more SNMP managers. By default no SNMP manager hosts are defined:

Figure 50 – SNMP Traps Table

To add a new trap host IP address for P-520 click the **Add** button and a new pop-up window **Add Trap Host IP Address** appears:

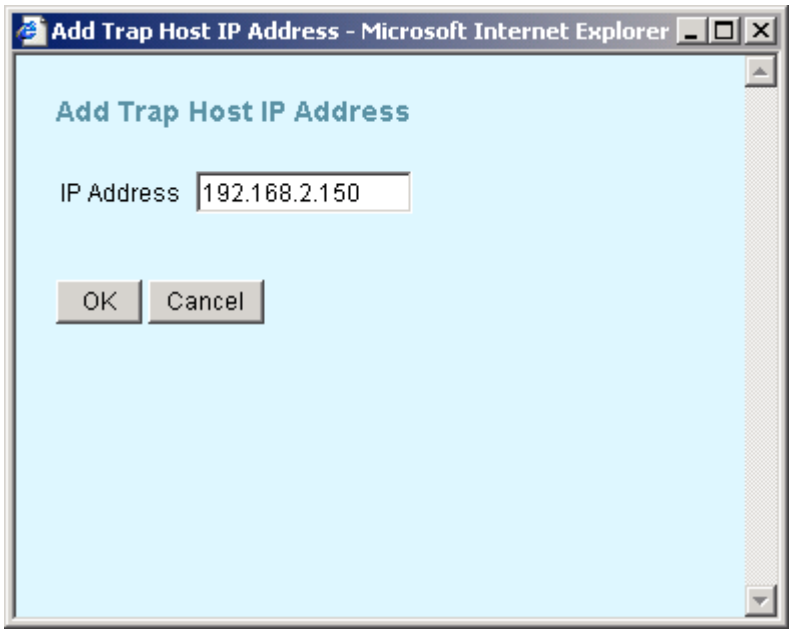


Figure 51 - Add Trap Host IP

IP Address – specify the SNMP manager IP address.

OK – saves added SNMP manager IP address into configuration.

Cancel – close the window without saving information.

Click the **Delete** button to delete desired SNMP traps hosts and a new pop-up window **Delete Trap Host IP addresses** appears. You can select the hosts' IP addresses that should be deleted as shown on the following example:

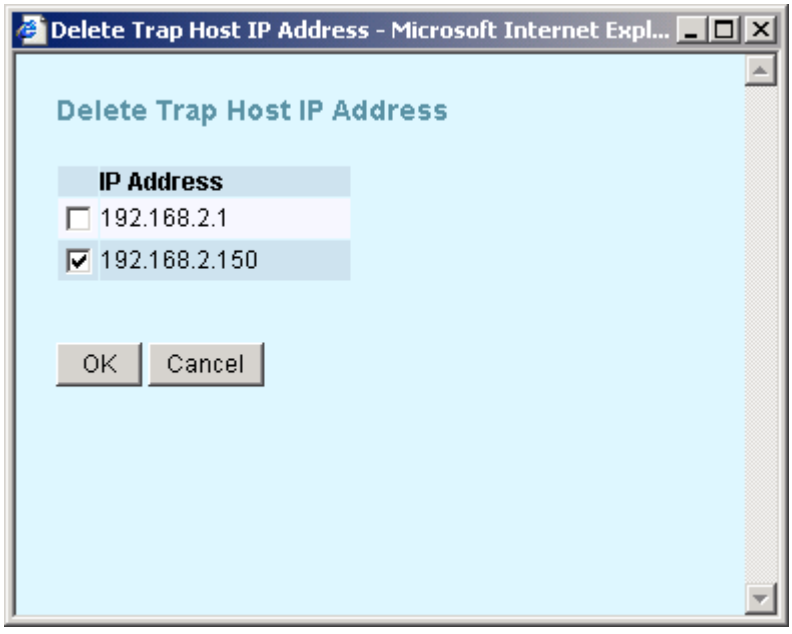


Figure 52 – Delete Trap Host IP

OK – removes selected SNMP manager IP addresses from the system.

Cancel – close the window without saving information.

Status

Status | Statistics/Usage | Status Overview

Use the **Status | Statistics/Usage | Status Overview** menu for a summary of status information of your access point.

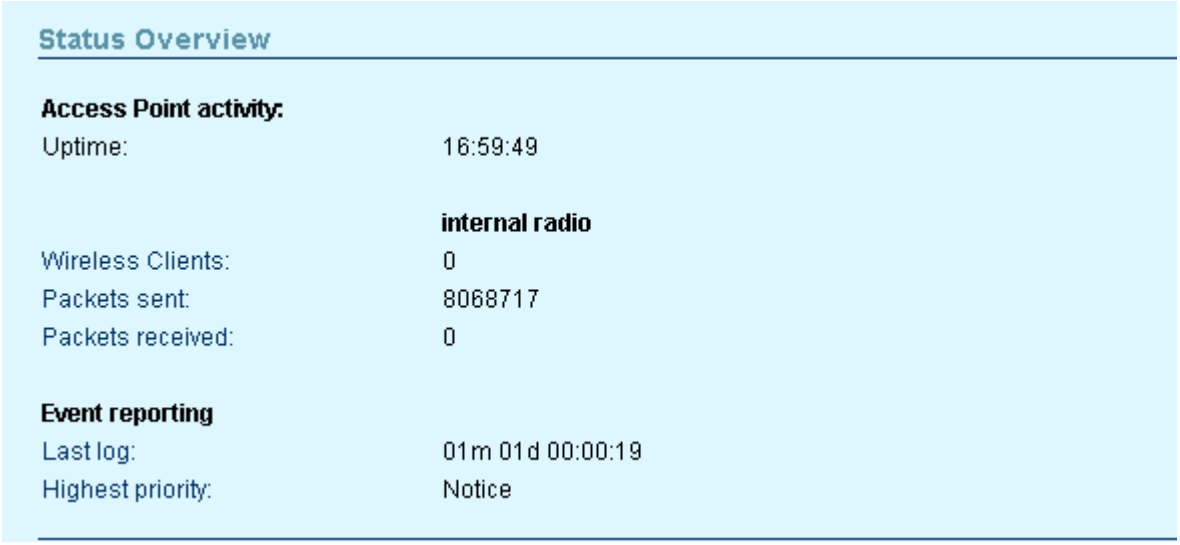


Figure 53 – Status Overview

Uptime – indicates the time, expressed in hours, minutes and seconds since last reboot [hours:minutes:seconds].

Wireless Clients – indicates the total number of currently connected client stations. Click on the hyperlink **Status | Clients | Wireless Clients** to see more details for individual clients.

Packets Sent – indicates the data volume transmitted to the wireless LAN since reboot.

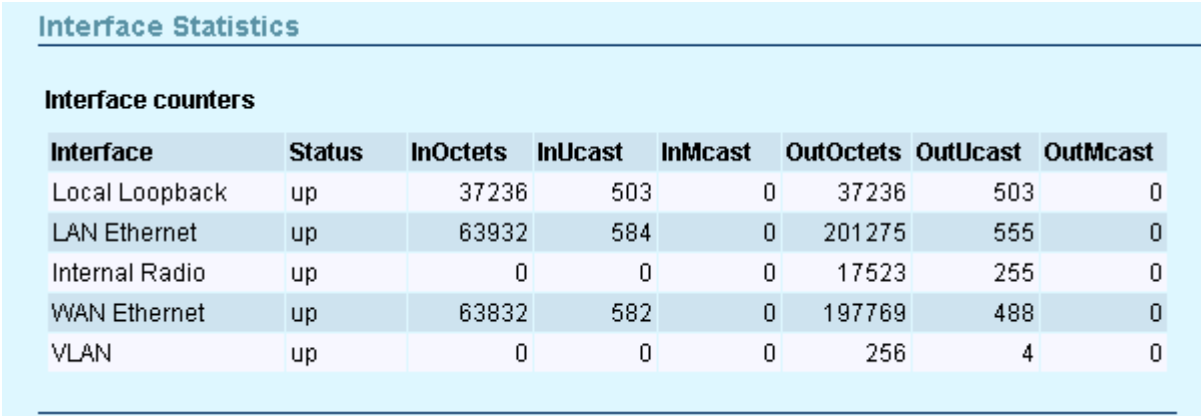
Packets Received – indicates the volume of data received since reboot.

Last Log – indicates the time when the access point has sent the most recent event message.

Highest Priority – shows the priority level of the last event [Emergency/Alert/Critical/Error/Warning/Notice/Info/Debug].

Status | Statistics/Usage | Interface Statistics

Use the **Status | Statistics/Usage | Interface Statistics** menu for a summary of interface statistics.



Interface	Status	InOctets	InUcast	InMcast	OutOctets	OutUcast	OutMcast
Local Loopback	up	37236	503	0	37236	503	0
LAN Ethernet	up	63932	584	0	201275	555	0
Internal Radio	up	0	0	0	17523	255	0
WAN Ethernet	up	63832	582	0	197769	488	0
VLAN	up	0	0	0	256	4	0

Figure 54 – Interface Statistics

Interface – indicates a unique name for each interface.

Status – shows the current operational state of the interface [up/down].

InOctets – indicates the amount of received bytes on the interface, including framing characters.

InUcast – totals unicast frames received at the port excluding discards.

InMcast – totals multicast frames received at the port excluding discards.

OutOctets – shows the total transmitted frames of the interface in bytes, including framing characters.

OutUcast – totals unicast frames transmitted from the port including discards.

OutMcast – totals multicast frames transmitted from the port including discards.

Status | Statistics/Usage | Wireless Statistics

Use the **Status | Statistics/Usage | Wireless Statistics** menu to view information regarding data traffic for the Wireless interface.

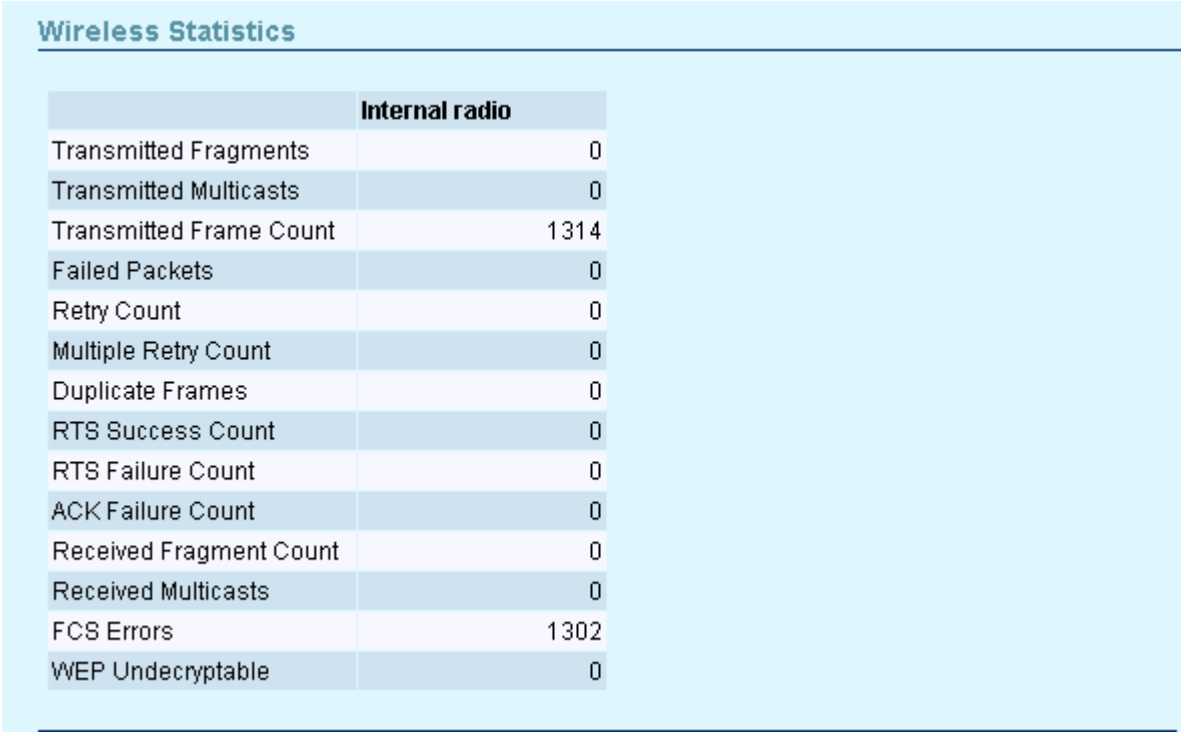


Figure 55 – Wireless Statistics

Transmitted Fragments – displays the total of transmitted fragmented frames.

Transmitted Multicasts – displays the total of transmitted multicast frames.

Transmitted Frame Count – displays count of successfully transmitted MSDU (MAC Service Data Units).

Failed Packets – displays the total of not transmitted MSDU.

Retry Count – displays the number of successfully transmitted MSDU after one or more retransmissions.

Multiple Retry Count – displays the number of successfully transmitted MSDU after more than one retransmissions.

Duplicate Frames – displays the total of duplicate frames.

RTS Success Count – displays the total of successfully received RTS packets.

RTS Failure Count – displays total of not received RTS packets.

ACK Failure Count – displays total of expected but not received ACK (acknowledgement) frames.

Received Fragment Count – displays total of each successfully received MPDU (MAC Protocol Data Unit) of type Data or Management.

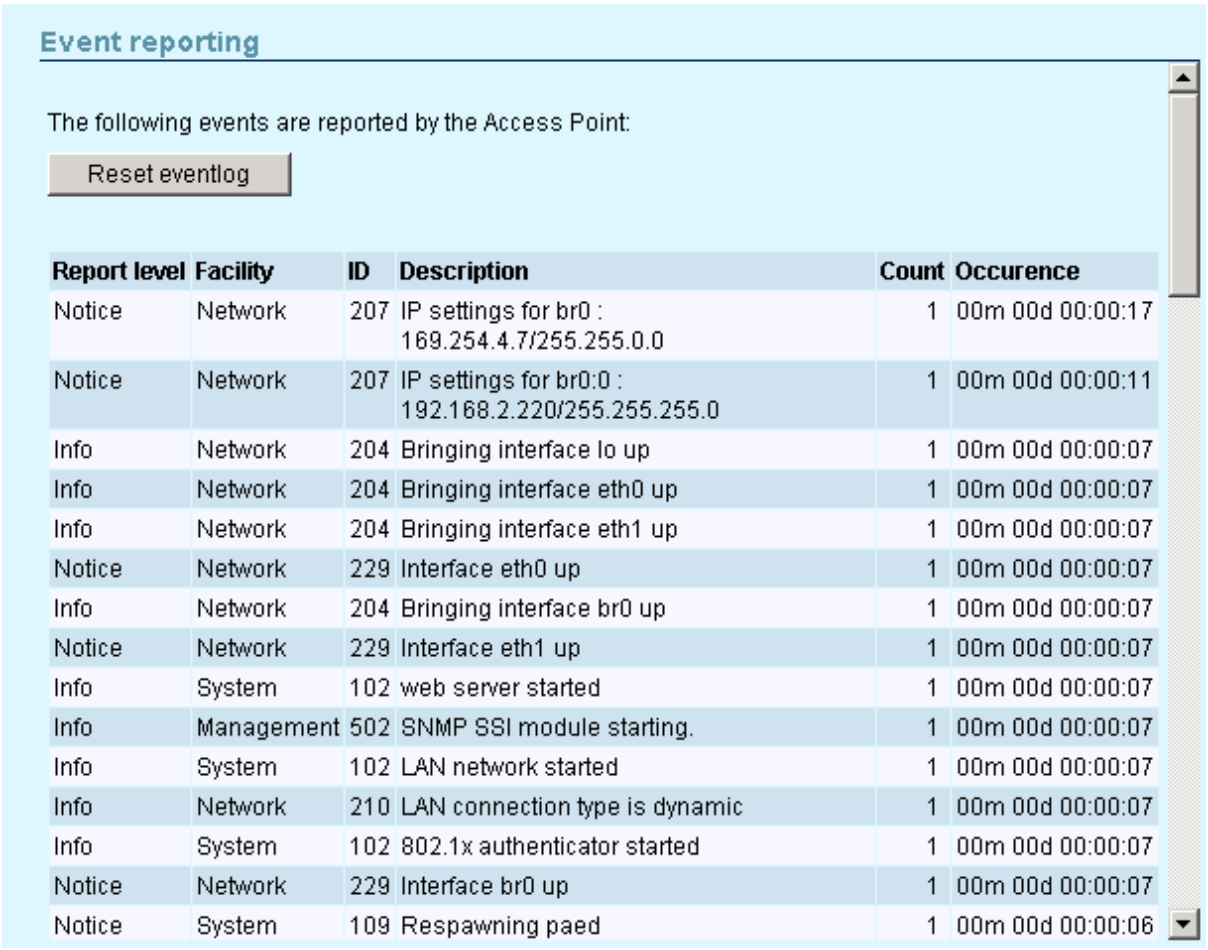
Received Multicasts Count – displays the total of MSDU, received with the multicast bit set in the destination MAC address.

FCS Errors – displays count of FCS (Frame Check Sequence) errors in received MPDU.

WEP Undecryptable – displays the number of not decrypted frames.

Status | Statistics/Usage | Event Reporting

The event reporting system informs about internal services and provides debug messages in case of malfunctions or network problems. The trace system can help operators to locate mis-configurations and system errors. Use the **Status | Statistics/Usage | Event Reporting** menu to view current syslog messages in case of troubleshooting of one of the services:



Report level	Facility	ID	Description	Count	Occurence
Notice	Network	207	IP settings for br0 : 169.254.4.7/255.255.0.0	1	00m 00d 00:00:17
Notice	Network	207	IP settings for br0:0 : 192.168.2.220/255.255.255.0	1	00m 00d 00:00:11
Info	Network	204	Bringing interface lo up	1	00m 00d 00:00:07
Info	Network	204	Bringing interface eth0 up	1	00m 00d 00:00:07
Info	Network	204	Bringing interface eth1 up	1	00m 00d 00:00:07
Notice	Network	229	Interface eth0 up	1	00m 00d 00:00:07
Info	Network	204	Bringing interface br0 up	1	00m 00d 00:00:07
Notice	Network	229	Interface eth1 up	1	00m 00d 00:00:07
Info	System	102	web server started	1	00m 00d 00:00:07
Info	Management	502	SNMP SSI module starting.	1	00m 00d 00:00:07
Info	System	102	LAN network started	1	00m 00d 00:00:07
Info	Network	210	LAN connection type is dynamic	1	00m 00d 00:00:07
Info	System	102	802.1x authenticator started	1	00m 00d 00:00:07
Notice	Network	229	Interface br0 up	1	00m 00d 00:00:07
Notice	System	109	Respawning paed	1	00m 00d 00:00:06

Figure 56 – Event Reporting

Reset Eventlog – delete all displayed logged messages.

Report Level – shows how important the event (or how critical the error) is [Emergency/Alert/Critical/Error/Warning/Notice/Info/Debug].

Facility – indicates the unique identifier of the facility that generated the event. A facility can be a hardware device, a protocol, or a module of the system software. [Kernel/User/Security/Clock/LogAudit/LogAlert/System/Network/Wlan/management]

ID – indicates an internal number for the event.

Description – indicates description of the event.

Count – indicates the number of times this event has occurred.

Occurrence – indicates time when this event has occurred, in months, days and hours:minutes:seconds since the access point was started.

Status | Clients | Wireless Clients

All clients currently connected to the P-520 access point are listed in the **Wireless Clients** table. Select the **Status | Clients | Wireless Clients** menu if you want to get statistics regarding wireless clients.

The wireless clients are listed by their **MAC address**, **Rate**, **Quality**, **RSSI**, **State** and **Age** parameters:

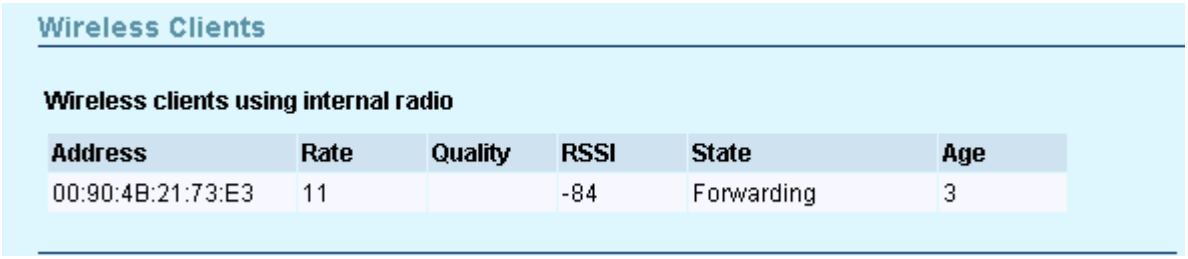


Figure 57 – Connected Wireless Clients

MAC Address – displays wireless client's MAC address.

Rate – displays the current data rate in Mbps.

Quality – displays an indicator for the quality of the client (not supported yet).

RSSI – displays the Received Signal Strength Indication (RSSI) in dBm of the client.

State – displays the connection status between client and AP [Disconnected/ DiscAndUlPreauth/ llAuthenticated/ llAuthAndUlPreauth/ Associated/ ulAuthenticated/ Key Distribution/Forwarding/ Rejected]. Only clients in the state Forwarding will be able to send/receive data to/from other devices.

Age – shows the age in seconds of the last information received from the client. The age is reset to 0 if any activity of this client is detected.

Status | Clients | Access Points

The page shows information about other wireless LANs in range. With this site survey administrator can scan for neighboring access points; check their operating channels, view MAC addresses, Data rates, and other parameters. The site survey does not interrupt any client or WDS connection.

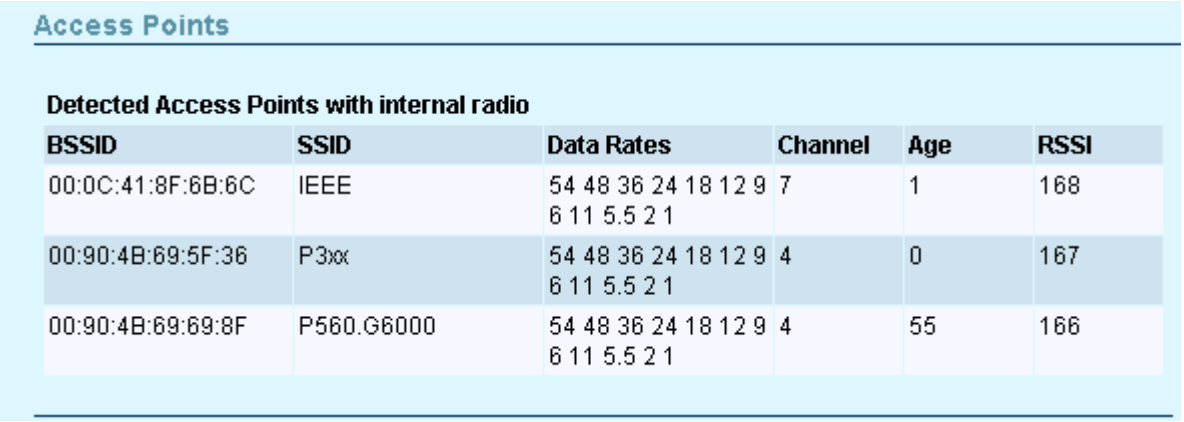


Figure 58 – Detected Access Points with Internal Radio

BSSID – displays the MAC address of the remote access point.

SSID – displays the network name (SSID) of the remote access point.

Data Rates – displays the range of data transmission rates supported by a device in megabits per second (Mbps).

Channel – displays the channel of the remote access point.

Age – shows the age in seconds of the last information received from the remote AP. The age is reset to 0 if any activity of this access point is detected.

RSSI – displays the Received Signal Strength Indication (RSSI) of the remote access point.

Status | Clients | WDS Links

This page displays status information about current bridge connections to other APs (WDS links).

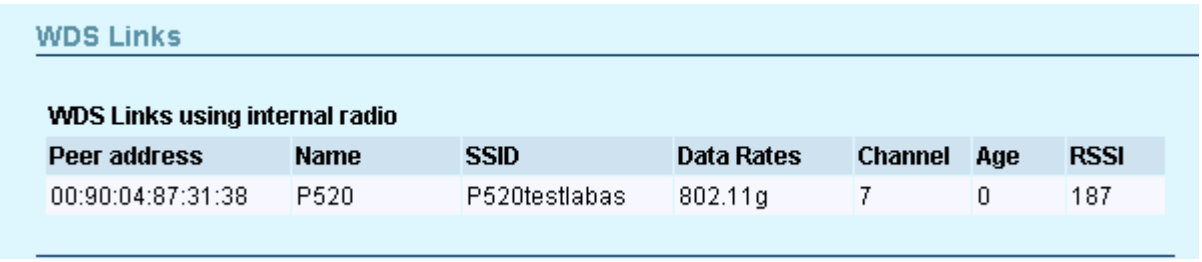


Figure 59 – WDS Link Statistics Table

Peer address – displays the MAC address of the remote WDS access point/bridge.

Name – shows the name of the WDS Link.

SSID – displays the SSID of the access point.

Data Rates – displays the data rates.

Channel – displays the radio channel for transmit and receive

Age – shows the age in seconds of the last information received from the remote AP. The age is reset to 0 if any activity of this access point is detected.

RSSI – displays the Received Signal Strength Indication (RSSI) of the remote access point.

Update

We recommend to regularly check for new Software updates on the Gemtek Systems website: http://www.gemtek-systems.com

To update your device firmware, use only the original Gemtek System firmware image and click the **update** button on main menu. New **Update Wizard** pop-up window appears.

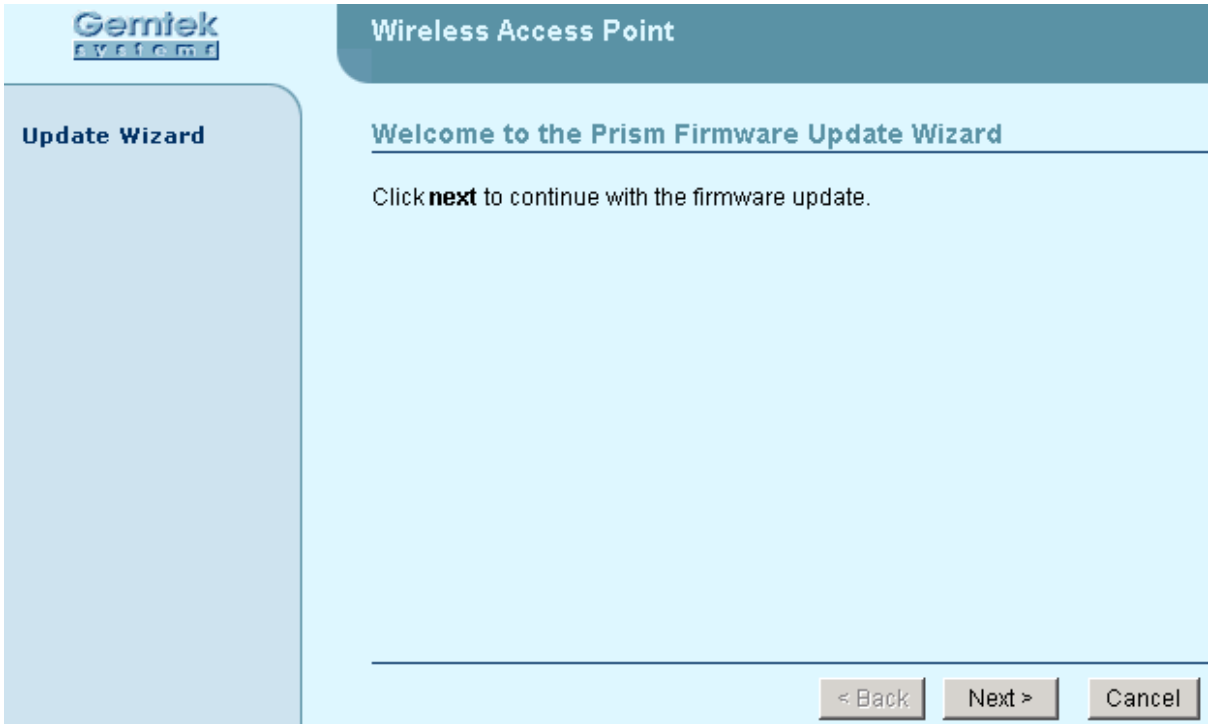


Figure 60 – Update Wizard

Next – click to continue the firmware update process.

Cancel – click to cancel the firmware update process.

To start update, click the **next** button and specify the full path to the new firmware image and click the **upload** button:

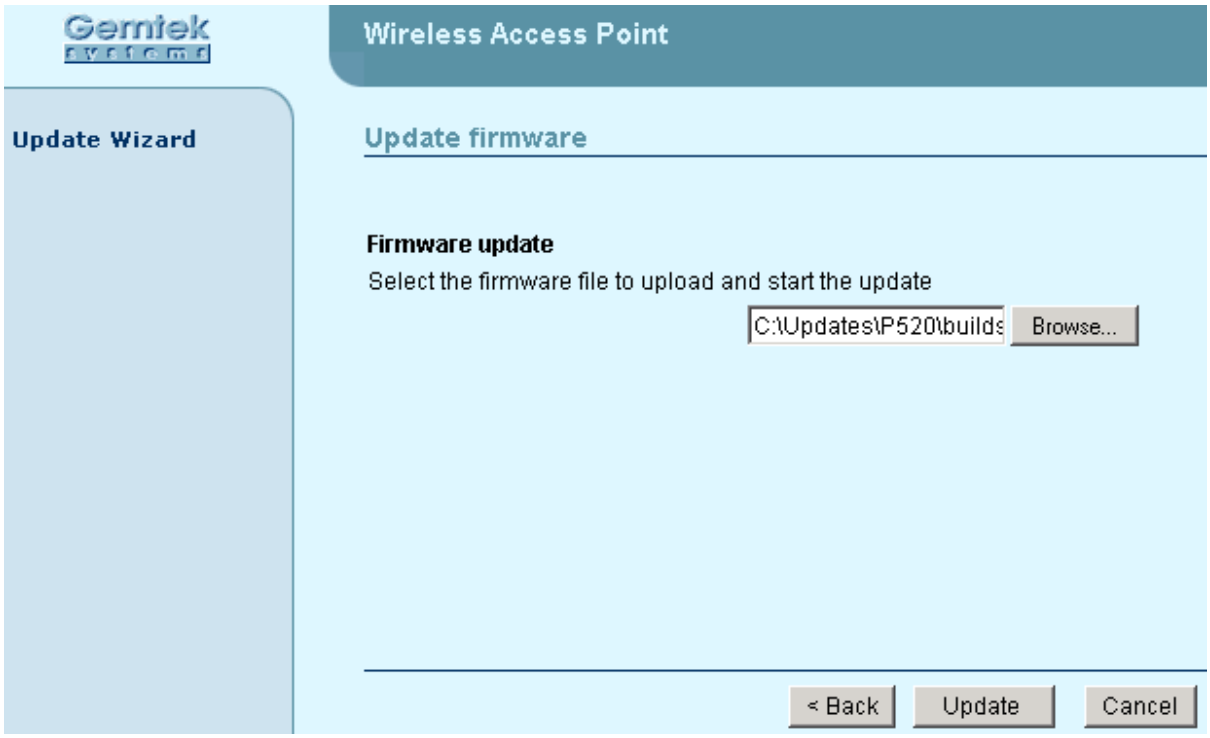


Figure 61 – New Firmware Upload

Browse – click the button to specify the new image location.

Update – upload with new firmware.

Cancel – cancel the upload process.

Back – return to main firmware update wizard page.

New firmware image is uploaded and system firmware update begins. New window with informational message and remaining time appears.

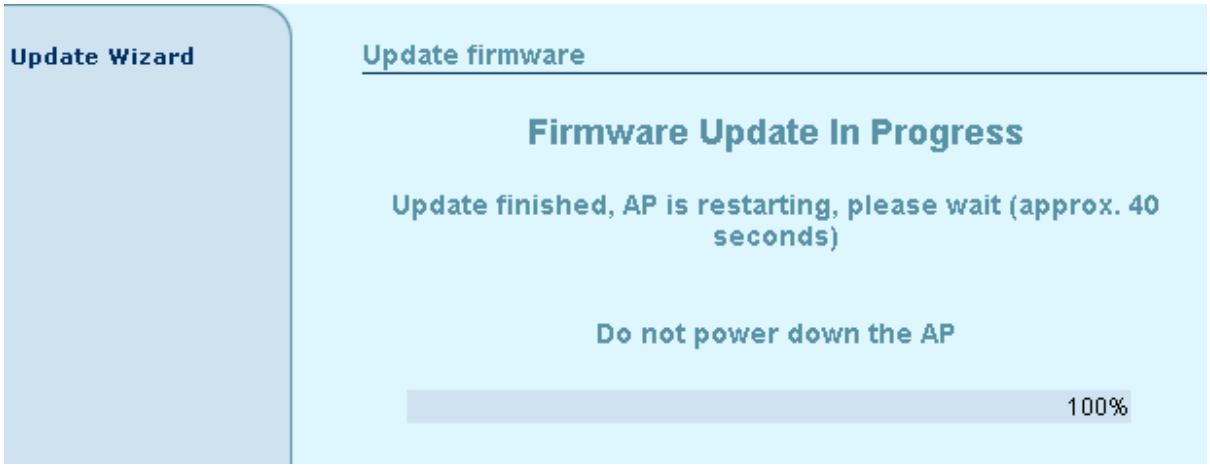


Figure 62 – Firmware Update Process

When the upload is completed successfully a confirmation message and the access point restarts.

Do not switch off and do not disconnect the P-520 from the power supply during the firmware update process as this can damage the device.

Chapter 5 – SNMP Management

Introduction

Another way to configure and monitor the access point (P-520) via a TCP/IP network is **SNMP** (Simple Network Management Protocol).

SNMP is an application layer protocol that facilitates the exchange of management information between network devices. It is part of the Transmission Control Protocol/Internet Protocol (TCP/IP) protocol suite. SNMP enables network administrators to manage network performance, find and solve network problems, and plan for network growth.

The SNMP agent and management information base (MIB) reside on the access point. To configure SNMP on the AP, you define the relationship between the Network Management System (NMS) and the SNMP agent (our AP). The SNMP agent contains MIB and **Gemtek Systems private MIB** variables whose values the SNMP manager can request or change. A NMS can get a value from an agent or store a value into the agent. The agent gathers data from the MIB, the repository for information about device parameters and network data. The agent can also respond to a manager's requests to get or set data.

In order to manage the device you have to provide your Network Management System software with adequate MIB files. Please consult your management software manuals on how to do that.

SNMP Versions

The access point supports the following versions of SNMP:

- **SNMPv1**—The Simple Network Management Protocol: A Full Internet Standard, defined in RFC 1157. (RFC 1157 replaces the earlier versions that were published as RFC 1067 and RFC 1098.) Security is based on community strings.

- **SNMPv2c**—The community-string based Administrative Framework for SNMPv2. SNMPv2c (the "C" stands for "community") is an Experimental Internet Protocol defined in RFC 1901, RFC 1905, and RFC 1906. SNMPv2c is an update of the protocol operations and data types of SNMPv2p (SNMPv2 Classic), and uses the community-based security model of SNMPv1.

Both SNMPv1 and SNMPv2c use a community-based form of security. The community of managers able to access the agent's MIB is defined by an IP address access control list and password.

The Access Controller implementation of SNMP supports all MIB II variables (as described in RFC 1213) and defines all traps using the guidelines described in RFC 1215.The traps described in this RFC are:

coldStart

A coldStart trap signifies that the SNMP entity, acting in an agent role, is reinitializing itself and that its configuration may have been altered.

WarmStart

A WarmStart trap signifies that the SNMP entity, acting in an agent role, is reinitializing itself

and that its configuration is unaltered.

authenticationFailure

An authenticationFailure trap signifies that the SNMP entity, acting in an agent role, has received a protocol message that is not properly authenticated.

linkDown

A linkDown trap signifies that the SNMP entity, acting in an agent role, recognizes a failure in one of the communication links represented in the agent's configuration.

linkUp

A linkUp trap signifies that the SNMP entity, acting in an agent role, recognizes that one of the communication links represented in the agent's configuration has come up.

SNMP Agent

The SNMP agent is integrated in your P-520 and responds to SNMP manager requests as follows:

- Get a MIB variable—The SNMP agent begins this function in response to a request from the SNMP manager. The agent retrieves the value of the requested MIB variable and responds to the manager with that value.
- Set a MIB variable—The SNMP agent begins this function in response to a message from the SNMP manager. The SNMP agent changes the value of the MIB variable to the value requested by the manager.

The SNMP agent also sends unsolicited trap messages to notify an SNMP manager that a significant event has occurred (e.g. authentication failures) on the agent.

SNMP Community Strings

SNMP community strings authenticate access to MIB objects and function as embedded passwords. In order for the SNMP manager to access the controller, the community string must match one of the two community string definitions on the controller. A community string can be as follows:

- **Read-only** – gives read access to authorized management stations to all objects in the MIB except the community strings, but does not allow write access.
- **Read-write** – gives read and write access to authorized management stations to all objects in the MIB, but does not allow access to the community strings.

The SNMP Read-write community string is also the administrator's password. If the password is changed the SNMP community string will be changed as well.

Use SNMP to Access MIB

As shown in the picture *Figure 63 – SNMP Network* SNMP agent gathers data from the MIB. The agent can send traps (notification of certain events) to the SNMP manager, which receives and processes the traps. Traps are messages alerting the SNMP manager to a condition on the network such as improper user authentication, restarts, link status (up or down), MAC address tracking, and so forth. The SNMP agent also responds to MIB-related queries sent by the SNMP manager in *get-request*, *get-next-request*, and *set-request* format.

Figure 63 – SNMP Network

Gemtek Systems Private MIB

In addition to standard SNMP MIBs the P-520 supports the **private Gemtek Systems MIB**. The private MIBs are enterprise specific and serve to extend the functionality of the standard MIBs. Private MIB identifies manageable objects and their properties that are specific to the managed device. MIBs let you manage device not only by using WEB or Command Line Interface but also using SNMP protocol. The descriptions and brief explanations of managed objects are available in the MIB file. The MIB file is a specially formatted text file. It is using the so-called ASN.1 standard syntax.

The Gemtek Systems private MIBs are the following:

- GemTek-Generic-Mib.mib
- GemTek-Mib.mib
- GemTek-Products-AP-Mib.mib
- GemTek-Products-Mib.mib
- GemTek-Traps-Mib.mib

Appendix

A) P-520 Operator Access Point Specification

Technical Data

Features			
▪ Theft protection system		▪ Power-over-Ethernet support ▪	
▪ IEEE 802.11g/b Access Point, Wi-Fi compliant		▪ Remote management, updates	
▪ WPA (PSK, TKIP, Rekeying)/WEP support		▪ Layer 2 isolation for security	
▪ Integrated high-gain diversity antennas		▪ Seamless roaming (IAPP) support	
▪ 802.1x security		▪ Virtual local area network support (VLAN)	
▪ RADIUS support		▪ Remote management via HTTP, SNMP (MIB II, Ethernet MIB, Bridge MIB, private MIB) Terminal	
▪ ACL (Access Control List)		▪ DHCP client	
Wireless			
Standard	IEEE 802.11b/g (2.4GHz ISM band), Wi-Fi compliant		
Data Rate	802.11b: 11, 5.5, 2, 1Mbps 802.11g: 54, 48, 36, 24, 18, 12, 9, 6		
Channels	Up to 14 channels selectable based on regulatory domain settings		
Transmit Power	0 - 20dBm (adjustable)		
Sensitivity	Data Rate	Sensitivity	Modulation
	54Mbps	-71dBm	64QAM/OFDM, 8% PER
	48Mbps	-73dBm	64QAM/OFDM, 8% PER
	36Mbps	-75dBm	16QAM/OFDM, 8% PER
	24Mbps	-78dBm	16QAM/OFDM, 8% PER
	18Mbps	-80dBm	QPSK/OFDM, 8% PER
	12Mbps	-82dBm	QPSK/OFDM, 8% PER
	11Mbps	-87dBm	CCK, 8% PER
	9Mbps	-84dBm	BPSK/OFDM, 8% PER
	6Mbps	-86dBm	BPSK/OFDM, 8% PER
	5.5Mbps	-89dBm	CCK, 8% PER
	2Mbps	-90dBm	DQPSK, 8% PER
	1Mbps	-92dBm	DBPSK, 8% PER
Antennas	Two integrated diversity antennas: 6dBi directional antenna vertical polarization & 4dBi horizontal polarized antenna		
Interface			
Ethernet Interface	10/100 base-T, RJ-45 Ethernet port for connection to LAN		
Serial Console Port	DB-9 connector (internal)		
Physical Specification			

Dimension	196mm x 142mm x 35 mm/ 7.6 x 5.5 x 1.4 (L x W x D)
Weight	350g / 0.771 lbs
Environment Specification	
Temperature	0°C to 45°C
Humidity	10% to 95%, non-condensing
Power Supply	
Power Adaptor	External AC/DC converter 100/230V to 5V DC/1.5A, 4.2W max.
Optional Power Supply	Power-over-Ethernet IEEE 802.3af compliant
Mechanical Specification	
Ruggedized and flame-resistant plastic housing and plate that allows for placement on a wall, theft protection	
LEDs	
3 LEDs	RF activity, LAN activity, Power
Management	
Interfaces	HTTP, SNMPv1 und SNMPv2 (MIB II, 802.11 MIB, private MIB), Terminal
Software Update	Remote Software Update via HTTP
Performance Monitor	Tx/Rx
Test	Integrated site survey
Reset	Remote reset/ Manufacturing reset
Warranty	
2 years	
Package Contents	
P-520 54Mb Operator Access Point	CD-ROM with software and documentation
Ethernet patch cable	100/230 Power Adapter
Wall mount plate	Unmount tool
Related Products	
Access Controllers:	G-6000, 4100 Public Access Controller
	P-560 54Mb Hotspot-in-a-Box
Client Adapters:	T-300 series (2.4 GHz, 11Mb)
PoE Switches:	E-820 8-port Power-over-Ethernet Switch
	E-110 Single-port PoE Feeder
Software:	S-1000 Network Management Suite

This table is for planning purposes only and is not intend to modify or supplement any specifications or warranties relating to Gemtek Systems products. Gemtek Systems may make changes to these specifications and descriptions at any time, without notice.

B) Regulatory Domain/Channels

Channels Identifiers	Frequency in MHz	USA, Canada (FCC)	ETSI	WORLD	France	China	Japan	Manual
1	2412	•	•	•	—	•	•	•
2	2417	•	•	•	—	•	•	•
3	2422	•	•	•	—	•	•	•
4	2427	•	•	•	—	•	•	•
5	2432	•	•	•	—	•	•	•
6	2437	•	•	•	—	•	•	•
7	2442	•	•	•	—	•	•	•
8	2447	•	•	•	—	•	•	•
9	2452	•	•	•	—	•	•	•
10	2457	•	•	•	•	•	•	•
11	2462	•	•	•	•	•	•	•
12	2467	—	•	—	•	•	•	•
13	2472	—	•	—	•	•	•	•
14	2484	—	—	—	—	—	•	•
Maximum Power Levels		30dBm	20dBm	20dBm	20dBm	20dBm	20dBm	30dBm

Mexico is included in the Americas regulatory domain; however, channels 1 through 8 are for indoor use only while channels 9 through 11 can be used indoors and outdoors. Users are responsible for ensuring that the channel set configuration complies with the regulatory standards of Mexico.

C) Factory Defaults Values for the P-520 Access Point

The following settings and parameters are the factory default for the 54Mb Operator Access Point model: P-520.

Configuration:

Identity	
Name	name
Location	location
Contact	contact information

Local Area Network:

Network Setup	
Dynamic IP	Selected
Static IP	Not Selected
Virtual LAN	
Use Virtual Local Network (VLAN)	Not selected
VLAN id	none

Wireless

Basic Wireless Settings	
Country	US
Regulatory Domain	FCC
Wireless Network Name (SSID)	P520
Band	Mixed
Radio Channel	6
PRISM Nitro™	Maximum
Broadcast SSID	Selected
Advanced Wireless Settings	
Operational Rate Set	82848B0C129618243048606C
Beacon Period	100
RTS Threshold	2347
Fragmentation Threshold	2346

Security

Wireless Security | Client Isolation	
Use Client Isolation	Not Selected
Wireless Security | Access Control List (ACL)	
Enable Access Control List	Not Selected

Wireless Security | RADIUS Servers	
Reauthentication Time	3600
No RADIUS servers are defined on the system in the default status	
Wireless Security | Wired Equivalency Privacy (WEP)	
Use WEP Security	Not selected
Wireless Security | 802.1X Security	
802.1X Security is not available because by default no RADIUS servers are on the system	
Wireless Security | Wi-Fi Protected Access (WPA)	
Disable WPA Security	Selected
Use WPA with Pre-shared Key	Not Selected
Use WPA with RADIUS server settings is not available because by default no RADIUS servers are on the system.	
Security | Management Security	
User name	admin (cannot be changed)
Password	admin01
System | SNMP Traps	
No SNMP traps on the system	
SNMP Community Strings	
Read-only	public (cannot be changed)
Read-write	admin01

D) Location ID and ISO Country Codes

This list states the **country names** (official short names in English) in alphabetical order as given in ISO 3166-1 **and** the corresponding **ISO 3166-1-alpha-2 code elements**.

It lists 239 official short names and code elements.

Location ID	Country	Location ID	Country
AF	Afghanistan	LI	Liechtenstein
AL	Albania	LT	Lithuania
DZ	Algeria	LU	Luxembourg
AS	American Samoa	MO	Macao
AD	Andorra	MK	Macedonia, the former Yugoslav republic of
AO	Angola	MG	Madagascar
AI	Anguilla	MW	Malawi
AQ	Antarctica	MY	Malaysia
AG	Antigua and Barbuda	MV	Maldives
AR	Argentina	ML	Mali
AM	Armenia	MT	Malta
AW	Aruba	MH	Marshall islands
AU	Australia	MQ	Martinique
AT	Austria	MR	Mauritania
AZ	Azerbaijan	MU	Mauritius
BS	Bahamas	YT	Mayotte
BH	Bahrain	MX	Mexico
BD	Bangladesh	FM	Micronesia, federated states of
BB	Barbados	MD	Moldova, republic of
BY	Belarus	MC	Monaco
BE	Belgium	MN	Mongolia
BZ	Belize	MS	Montserrat
BJ	Benin	MA	Morocco
BM	Bermuda	MZ	Mozambique
BT	Bhutan	MM	Myanmar
BO	Bolivia	NA	Namibia
BA	Bosnia and Herzegovina	NR	Nauru
BW	Botswana	NP	Nepal
BV	Bouvet island	NL	Netherlands
BR	Brazil	AN	Netherlands Antilles
IO	British Indian ocean territory	NC	New Caledonia
BN	Brunei Darussalam	NZ	New Zealand
BG	Bulgaria	NI	Nicaragua
BF	Burkina Faso	NE	Niger
BI	Burundi	NG	Nigeria

KH	Cambodia	NU	Niue
CM	Cameroon	NF	Norfolk island
CA	Canada	MP	Northern Mariana islands
CV	Cape Verde	NO	Norway
KY	Cayman islands	OM	Oman
CF	Central African republic	PK	Pakistan
TD	Chad	PW	Palau
CL	Chile	PS	Palestinian territory, occupied
CN	China	PA	Panama
CX	Christmas island	PG	Papua new guinea
CC	Cocos (keeling) islands	PY	Paraguay
CO	Colombia	PE	Peru
KM	Comoros	PH	Philippines
CG	Congo	PN	Pitcairn
CD	Congo, the democratic republic of the	PL	Poland
CK	Cook islands	PT	Portugal
CR	Costa Rica	PR	Puerto Rico
CI	Côte d'ivoire	QA	Qatar
HR	Croatia	RE	Réunion
CU	Cuba	RO	Romania
CY	Cyprus	RU	Russian federation
CZ	Czech republic	RW	Rwanda
DK	Denmark	SH	Saint Helena
DJ	Djibouti	KN	Saint Kitts and Nevis
DM	Dominica	LC	Saint Lucia
DO	Dominican republic	PM	Saint Pierre and Miquelon
EC	Ecuador	VC	Saint Vincent and the grenadines
EG	Egypt	WS	Samoa
SV	El Salvador	SM	San Marino
GQ	Equatorial guinea	ST	Sao tome and Principe
ER	Eritrea	SA	Saudi Arabia
EE	Estonia	SN	Senegal
ET	Ethiopia	SC	Seychelles
FK	Falkland islands (malvinas)	SL	Sierra Leone
FO	Faroe islands	SG	Singapore
FJ	Fiji	SK	Slovakia
FI	Finland	SI	Slovenia
FR	France	SB	Solomon islands
GF	French Guiana	SO	Somalia
PF	French Polynesia	ZA	South Africa
TF	French southern territories	GS	South Georgia and the south sandwich islands

GA	Gabon	ES	Spain
GM	Gambia	LK	Sri Lanka
GE	Georgia	SD	Sudan
DE	Germany	SR	Suriname
GH	Ghana	SJ	Svalbard and Jan Mayan
GI	Gibraltar	SZ	Swaziland
GR	Greece	SE	Sweden
GL	Greenland	CH	Switzerland
GD	Grenada	SY	Syrian Arab republic
GP	Guadeloupe	TW	Taiwan, province of china
GU	Guam	TJ	Tajikistan
GT	Guatemala	TZ	Tanzania, united republic of
GN	Guinea	TH	Thailand
GW	Guinea-Bissau	TL	Timor-leste
GY	Guyana	TG	Togo
HT	Haiti	TK	Tokelau
HM	Heard island and McDonald islands	TO	Tonga
VA	Holy see (Vatican city state)	TT	Trinidad and Tobago
HN	Honduras	TN	Tunisia
HK	Hong Kong	TR	Turkey
HU	Hungary	TM	Turkmenistan
IS	Iceland	TC	Turks and Caicos islands
IN	India	TV	Tuvalu
ID	Indonesia	UG	Uganda
IR	Iran, Islamic republic of	UA	Ukraine
IQ	Iraq	AE	United Arab emirates
IE	Ireland	GB	United kingdom
IL	Israel	US	United states
IT	Italy	UM	United states minor outlying islands
JM	Jamaica	UY	Uruguay
JP	Japan	UZ	Uzbekistan
JO	Jordan	VU	Vanuatu
KZ	Kazakhstan		Vatican city state see holy see
KE	Kenya	VE	Venezuela
KI	Kiribati	VN	Viet nam
KP	Korea, democratic people's republic of	VG	Virgin islands, British
KR	Korea, republic of	VI	Virgin islands, u.s.
KW	Kuwait	WF	Wallis and Futuna
KG	Kyrgyzstan	EH	Western Sahara
LA	Lao people's democratic republic	YE	Yemen
LV	Latvia	YU	Yugoslavia

LB	Lebanon		Zaire see Congo, the democratic republic of the
LS	Lesotho	ZM	Zambia
LR	Liberia	ZW	Zimbabwe
LY	Libyan Arab Jamahiriya		

Glossary

Symbols:

10BASET 10 Mbps/baseband/twisted pair. The IEEE standard for twisted pair Ethernet.
802.11b The IEEE standards for the definition of the Wireless high-speed (11Mbit) protocol for wireless communication.

A

Authorization the process of determining what types of activities a user is permitted to undertake. Usually, authorization is in the context of authentication: once you have authenticated a user, they may be authorized for different types of access or activity.

Authentication - Authentication is the process of determining whether someone or something is, in fact, who or what it is declared to be.

B

backbone The primary connectivity mechanism of a hierarchical distributed system. All systems, which have connectivity to an intermediate system on the backbone, are assured of connectivity to each other. This does not prevent systems from setting up private arrangements with each other to bypass the backbone for reasons of cost, performance, or security.

bandwidth Technically, the difference, in Hertz (Hz), between the highest and lowest frequencies of a transmission channel. However, as typically used, the amount of data that can be sent through a given communications circuit. For example, typical Ethernet has a bandwidth of 100Mbps.

bps bits per second. A measure of the data transmission rate.

D

Datagram Self-contained, independent entity of data carrying sufficient information to be routed from the source to the destination computer without reliance on earlier exchanges between this source and destination computer and the transporting network." a self-contained, independent entity of data carrying sufficient information to be routed from the source to the destination computer without reliance on earlier exchanges between this source and destination computer and the transporting network. The term has generally been replaced by “packet”.

DHCP Dynamic Host Configuration Protocol. A service that lets clients on a LAN request configuration information, such as IP host addresses, from a server.

DNS Domain Name System. The distributed name/address mechanism used in the Internet. It comprises distributed online databases that contain mappings between human-readable names and IP addresses, and servers, which provide translation services to client applications.

Domain A part of the DNS naming hierarchy. Syntactically, an Internet domain name consists of a sequence of names (labels) separated by periods (dots), e.g., “machine.company.com”. See **DNS**.

E

Ethernet A common, 10Mbps local area network technology invented by Xerox Corporation at the Palo Alto Research Center. Ethernet is a best-effort delivery system that uses CSMA/CD technology. Ethernet can be run over thin wire coaxial cable (10BASE2), thick wire coaxial cable (10BASE5), twisted pair cable (10BASET), or fiber optic cable.

EIRP Effective Isotropic Radiated Power Technical value that evaluates the strength of receive signals

EPROM – EPROM (erasable programmable read-only memory) is programmable read-only memory (programmable ROM) that can be erased and re-used.

F

filter A device that selectively sorts signals and passes through a desired range of signals while suppressing the others. This kind of filter is used to suppress noise or to separate signals into bandwidth channels.

firewall A system or combination of systems that enforces a boundary between two or more networks.

FLASH A new memory technology, which combines the nonvolatile features of EPROM's with the easy in-system reprogramming of conventional volatile RAM. See **EPROM**.

G

gateway The original Internet term for what is now called router or more precisely, IP router. In modern usage, the term "gateway" and "application gateway" refers to systems, which perform translation from some native protocol, or physical data format to another. Examples include electronic mail gateways, which translate between X.400 and RFC 822 mail message formats. See **router**.

H

host An (end-user) computer system that connects to a network, such as a PC, minicomputer of mainframe.

hotspot A hotspot is wireless public access system that allows subscribers to connect to a wireless network in order to access the Internet or other devices, such as printers. Hotspots are created by WLAN access points, installed in public venues. Common locations for public access are hotels, airport lounges, railway stations or coffee shops.

HTTPS (Hypertext Transfer Protocol over Secure Socket Layer, or HTTP over SSL) is a Web protocol developed by Netscape and built into its browser that encrypts and decrypts user page requests as well as the pages that are returned by the Web server. HTTPS is really just the use of Netscape's Secure Socket Layer (SSL) as a sublayer under its regular HTTP application.

I

ICMP Internet Control Message Protocol. The TCP/IP protocol used to handle errors and control messages at the IP layer. ICMP is part of the IP protocol. Gateways, routers and hosts use ICMP to send reports of problems about datagrams back to the original source that sent the datagram.

interface One of the physical ports on the router, including the Ethernet and asynchronous ports.

interface type The type (Ethernet or Point-to-Point) of one of the interfaces on the router.

internet A collection of networks interconnected by a set of routers, which allow them to function as a single, large virtual network.

Internet (note the capital "I") The largest internet in the world consisting of large national backbone networks (such as MILNET, NSFNET, and CREN) and a myriad of regional and local campus networks all over the world. The Internet is a multiprotocol network, but generally carries TCP/IP.

Internet address See **IP address**.

Internet Protocol See **IP**.

ISP Internet service provider. A company that provides Internet - related services. Most importantly, an ISP provides Internet access services and products to other companies and consumers.

IP Internet Protocol. The network layer protocol for the TCP/IP protocol suite. It is a connectionless, best-effort packet switching protocol.

IP address A 32-bit address assigned to hosts using TCP/IP. The address specifies a specific connection to a network, not the host itself. See dotted decimal notation.

L

LAN Local Area Network. Any physical network technology (such as Ethernet) that operates at high speed (typically 10 Mbit per second or more) over short distances (up to a few kilometers). See **WAN**.

LED Light Emitting Diode. A luminous indicator.

M

MAC (Media Access Control) The unique hardware number of a device connected to a shared media. On an Ethernet it is the same interface as the Ethernet address.

metric A concept used to describe the cost of a route across a network, the distance to the destination at the remote end of the route, or the capacity of the route.

MIB A management information base (MIB) is a formal description of a set of network objects that can be managed using the Simple Network Management Protocol (SNMP). There are MIBs (or more accurately, MIB extensions) for each set of related network entities that can be managed.

N

name resolution The process of mapping a name into the corresponding address. See **DNS**.

NAT Network Address Translation, an Internet standard that enables a local-area network (LAN to use one set of IP addresses for internal traffic and a second set of addresses for external traffic. A NAT box located where the LAN meets the Internet makes all necessary IP address translations. NAT is used for two main tasks – to provide a type of firewall by hiding internal IP addresses and enable a company to use more internal IP addresses. Since they're used internally only, there's no possibility of conflict with IP addresses used by other companies and organizations.

network A computer network is a data communications system, which interconnects computer systems at various different sites. A network may be composed of any combination of LANs or WANs.

network address The network portion of an IP address. For a class A network, the network address is the first byte of the IP address. For a class B network, the network address is the first two bytes of the IP address. For a class C network, the network address is the first three bytes of the IP address. In each case, the remainder is the host address. In the Internet, assigned network addresses are globally unique. See **IP address**.

node An addressable device attached to a computer network. See **host**, **router**.

P

packet The unit of data sent across a network. "Packet" is a generic term used to describe units of data at all levels of the protocol stack, but it is most correctly used to describe application data units. See **datagram**, **frame**.

policy Organization-level rules governing acceptable use of computing resources, security practices, and operational procedures.

POP3: POP3 (Post Office Protocol 3) is the most recent version of a standard protocol for receiving e-mail. POP3 is a client/server protocol in which e-mail is received and held for you by your Internet server. Periodically, you (or your client e-mail receiver) check your mail-box on the server and download any mail. POP3 is built into the Netmanage suite of Internet products and one of the most popular e-mail products, Eudora. It's also built into the Netscape and Microsoft Internet Explorer browsers.

PPP: PPP (Point-to-Point Protocol) is a protocol for communication between two computers using a serial interface, typically a personal computer connected by phone line to a server. PPP uses the Internet protocol (IP) (and is designed to handle others). It is sometimes considered a member of the TCP/IP suite of protocols. Relative to the Open Systems Interconnection (OSI) reference model, PPP provides layer 2 (data-link layer) service. Essentially, it packages your computer's TCP/IP packets and forwards them to the server where they can actually be put on the Internet.

PPP is a full-duplex protocol that can be used on various physical media, including twisted pair or fiber optic lines or satellite transmission. It uses a variation of High Speed Data Link Control (HDLC) for packet encapsulation.

PPP is usually preferred over the earlier de facto standard Serial Line Internet Protocol (SLIP) because it can handle synchronous as well as asynchronous communication. PPP can share a line with other users and it has error detection that SLIP lacks. Where a choice is possible, PPP is preferred.

PPPoE: PPPoE (Point-to-Point Protocol over Ethernet) is a specification for connecting multiple computer users on an Ethernet local area network to a remote site through common customer premises equipment, which is the telephone company's term for a modem and similar devices. PPPoE can be used to have an office or building-full of users share a common Digital Subscriber Line (DSL), cable modem, or wireless connection to the Internet. PPPoE combines the Point-to-Point Protocol (PPP), commonly used in dialup connections, with the Ethernet protocol, which supports multiple users in a local area network. The PPP protocol information is encapsulated within an Ethernet frame.

PPPoE has the advantage that neither the telephone company nor the Internet service provider (ISP) needs to provide any special support. Unlike dialup connections, DSL and cable modem connections are "always on." Since a number of different users are sharing the same physical connection to the remote service provider, a way is needed to keep track of which user traffic should go to and which user should be billed. PPPoE provides for each user-remote site session to learn each other's network addresses (during an initial exchange called "discovery"). Once a session is established between an individual user and the remote site (for example, an Internet service provider), the session can be monitored for billing purposes.

PPTP: Point-to-Point Tunneling Protocol (PPTP) is a protocol (set of communication rules) that allows corporations to extend their own corporate network through private "tunnels" over the public Internet. Effectively, a corporation uses a wide-area network as a single large local area network. This kind of interconnection is known as a virtual private network (VPN).

port The abstraction used by Internet transport protocols to distinguish among multiple simultaneous connections to a single destination host. A port is a transport layer demultiplexing value. Each application has a unique port number associated with it. It is also used to refer to one of the physical network connectors on the router.

protocol A formal description of message formats and the rules two computers must follow to exchange those messages. Protocols can describe low-level details of machine-to-machine interfaces (e.g., the order in which bits and bytes are sent across a wire) or high-level exchanges between allocation programs (e.g., the way in which two programs transfer a file across the Internet).

Q

QOS Quality of Service. Transmission system qualities measure in terms of reliability and availability.

R

RADIUS (Remote Authentication Dial-In User Service) is a client/server protocol and software that enables remote access servers to communicate with a central server to authenticate dial-in users and authorize their access to the requested system or service. RADIUS allows a company to maintain user profiles in a central database that all remote servers can share. It provides better security, allowing a company to set up a policy that can be applied at a single administered network point. Having a central service also means that it's easier to track usage for billing and for keeping network statistics.

route The path that network traffic takes from the source to the destination. It may include many gateways, routers, hosts and physical networks.

route table A table listing information about routes to other hosts or networks, such as the remote network or host address, the interface down which the route exists, the distance to the remote address and the cost of sending data over the route.

router A system responsible for making decisions about which of several paths network (or Internet) traffic will follow. To do this it uses a routing protocol to gain information about the network, and algorithms to choose the best route based on several criteria known as “routing metrics”.

Router On the Internet, a router is a device or, in some cases, software in a computer, that determines the next network point to which a packet should be forwarded toward its destination. The router is connected to at least two networks and decides which way to send each information packet based on its current understanding of the state of the networks it is connected to.

S

server A network device that provides services to client stations. Examples include file servers and print servers.

service A term used with the router to refer to a connection to another port on (another) router, used to access dialup modems, hosts that do not support TCP/IP and other asynchronous devices.

SNMP A Simple Network Management Protocol. The Internet standard protocol developed to manage nodes on an IP network. See **MIB**.

subnet A portion of a network, which may be a physically independent network segment, which shares a network address with other portions of the network and is distinguished by a subnet number. A subnet is to a network what a network is to an internet.

subnet address The subnet portion of an IP address. In a subnetted network, the host portion of an IP address is split into a subnet portion and a host portion using an address or subnet mask. See subnet mask, IP address and network address.

subnet mask A bit mask used to select bits from an Internet address for subnet addressing. The mask is 32 bits long and selects the network portion of the Internet address and one or more bits of the local portion. Sometimes called address mask.

T

TCP Transmission Control Protocol. The TCP/IP standard transport layer protocol in the Internet suite of protocols, providing reliable, connection-oriented, full-duplex streams. It uses IP for delivery.

Telnet The virtual terminal protocol in the TCP/IP suite of protocols, which allows users of one host to log into a remote host and interact as normal terminal users of that host.

topology A network topology shows the computers and the links between them. A network layer must know the current network topology to be able to route packets to their final destination.

U

UDP User Datagram Protocol. A transport layer protocol in the TCP/IP suite of protocols. UDP, like TCP, uses IP for delivery; however, unlike TCP, UDP provides for exchange of datagrams without acknowledgements or guaranteed delivery.

URL Uniform Resource Locator. A standard format for specifying the name, type and location of documents and resources on an Internet. The syntax is type://host.domain :port/path/filename, where type specifies the type of document or resource (e.g. http is a file on a WWW server; file is a file on an anonymous FTP server; Telnet is a connection to a Telnet-based service). See **WWW**.

W

WAN Wide Area Network. Any physical network technology that spans large geographic distances. WANs usually operate a slower speeds than LANs. See **LAN**.

Wi-Fi is short for ***wi****reless* ***fi****delity* and is another name for IEEE 802.11b. It is a registered trademark of Wi-Fi Alliance. "Wi-Fi" is used in place of 802.11b in the same way that "Ethernet" is used in place of IEEE 802.3. Products certified as Wi-Fi by Wi-Fi Alliance are interoperable with each other even if they are from different manufacturers. A user with a Wi-Fi product can use any brand of access point with any other brand of client hardware that is built to the Wi-Fi standard.

WWW World Wide Web. A hypertext-based, distributed information system based on client - server architecture. Web browsers (client applications) request documents from Web servers. Documents may contain text, graphics and audiovisual data, as well as links to other documents and services. Web servers and documents are identified by URLs (Uniform Resource Locators). See **URL**.

Index

Q

R

S

T

U

V

W